INGRAM MICRO SECURITY

Eyesight Report

XXXXXX

27 September 2021

confidential

Document details

Document

Title	Eyesight Report
Subject	xxxxxxxxxx
Target URL	xxxxxx.pl

Document Version

Version	Date	Changes	Author (s)
0.1	27 September 2021	Initial Version	Aswin Gopalakrishnan
1.0	27 September 2021	Internally Reviewed Final Version	Sebastian Eitel, Brian Verburg, Hugo Inigo

Contact information

Name	TBD
Function	TBD
E-mail address	TBD

Disclaimer

Ingram Micro Cyber Security Center of Excellence ©.

This document is provided by Ingram Micro Cyber Security Team and classified as confidential.

Executive Summary

The Cyber Security Center of Excellence of IngramMicro conducted a comprehensive public discovery report (PDR) of xxxxxx by gathering data from public sources such as those available on the Internet. The intelligence information was gathered, analysed and converted into a human readable form, which was reviewed, and risks identified. The objective of this assessment is to provide the xxxxxx management team an understanding of the domain information exposed to the public Internet.

Scope

The test scope for this engagement is: **xxxxxxxxx**

Testing was performed on 27.September 2021. Additional days were utilized to produce the report.

Assessment was performed using industry-standard open source intelligence tools and frameworks, including Shodan, Censis.io, Fierce, Tidos Framework, the Google-Dorks, Alienware Threat intelligence, Recon-ng , theHarvester, Metagoofil, SpiderFoot, Recorded-Future and Maltego.

Limitations

It is not within the scope of this engagement to evaluate the security posture of the target. The primary objective is to gather relevant information about the domain that may be utilised by hackers for conducting cyber-attacks. None of the identified risks were exploited during this engagement; these risks should only be treated as plausible threats with a likelihood of causing damage to the organisation.

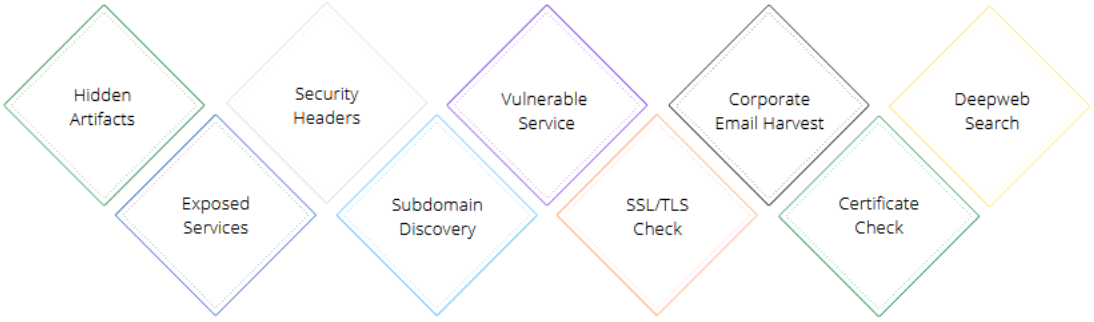
The findings in the report are not conclusive, as the results are generated automatically using a collection of industry-standard open source intelligence (OSINT) tools and frameworks. For more conclusive and thorough investigation of the domain or network, refer to other Cyber Security Service offerings of Ingram Micro. For more information, please reach out to your channel partner.

Methodology

The intelligence information gathered from publicly available resources are evaluated to identify risks and threats on any given target. These resources include search engines, paste sites, blogs, social networking sites, metadata and digital files, dark web resources geolocation, and anything available in the public internet.

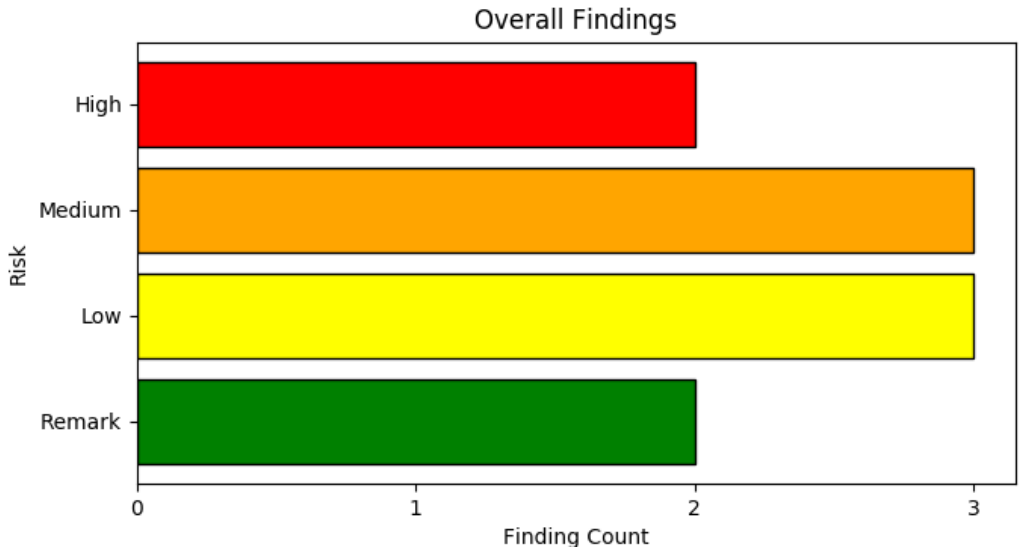
The PDR (aka OSINT) assessment distinguishes from other form of assessments because the collected information is legally accessible to the public without breach of any copyright or privacy laws. Therefore, the information accumulated, and methodologies used retrieve them strictly adhere to the legal and compliance regulations at Ingram Micro, and pose no risk to the customer's systems or information.

The image below describes the tactical intelligence gathered in this report:



Outcome

The following provide an overview of the findings identified during the engagement.



Since the business impact is hard to evaluate by us, all findings and their corresponding risks must be interpreted by Pl in the context of the system.

The outcome of the Eyesight investigation is below:

High finding one: An effective authentication mechanism was missing on the domain. Email is one of most dominant modes of communication in today's world and because it was not designed with security in mind, adversaries often exploit its security flaws to their advantage. One common attack form is email spoofing wherein an attacker sends malicious email posing as a legitimate user of the organisation.

High finding two: Eyesight discovered outdated software(s) installed on the target server(s) associated with the domain. Outdated software(s) are unmaintained and cannot integrate with new applications, nor can it run smoothly on new platforms. As a result, outdated software might not be able to withstand an up-to-date cyber-attack thereby making the systems more vulnerable to ransomware attacks, malware and data breaches. This risk affects confidentiality, integrity and availability of the application.

Medium finding one: Eyesight was able to discover corporate email accounts in the database of hacked websites and leaked passwords. This may be due to the data breach which occurred in the recent past or caused due to an ongoing cyber-attack. A data breach occurs when a hacker gains access to the data-base of a service or company which contains users' private information. This information can range from user-names and pass-words to social security numbers, addresses and even payment details. An adversary might use the compromised accounts for a variety of purposes including spam, phishing, fraud, and identity theft attacks. The risk affects the confidentiality of user data.

Medium finding two: Modern browsers have security features in place that can improve web application security to protect against clickjacking, cross-site scripting, and other common attacks. These are referred to as HTTP headers and they provide an extra layer of security by restricting behaviours that the browser and server allow once the web application is running. Eyesight discovered that the application server does not enforce relevant security headers to protect modern browsers from encountering vulnerabilities. These findings impact confidentiality, integrity and availability of data.

Medium finding three: Expired SSL certificate does not offer any protection to the customer data. By installing an SSL certificate on your website's server, it allows you to host it over secure, encrypted connections between your site and its visitors. Moreover these certificates produce scary browser warnings that drive customers due to the fear that the website does not secure their credentials. Both brand reputation and customer trust are damaged here. The risk affects confidentiality and Integrity of user data.

Low finding one: Open ports increase the risk of a data breach as these are doorways to the organisation's secure perimeter. The services listening on these ports may be misconfigured, unpatched, vulnerable to exploits, or may have poor network security rules. An attacker may exploit the services hosted on these ports and gain access to the internal network of the organisation.

Low finding two: Revealing system information makes life easier for an attacker and gives them a playbook of vulnerabilities they can probe for in the internet. Eyesight upon evaluating the responses from the server identifies sensitive information about the installed technologies. This information may be used by an attacker to search for known or common misconfiguration that would assist in more complex cyber-attacks. When a zero-day vulnerability is discovered, hackers will immediately find ways to exploit them and if the website leaks information about the technology it uses, the organisation may become victim of an automated cyber-attack.

Low finding three: Using depreciated SSL protocols places the integrity of the data at risk. Since the majority of modern browsers and clients implement TLS 1.2, a non-technical user would think that they should be safe. Unfortunately, this is not true and having support for earlier versions of TLS poses a security threat to users of even modern clients and servers. Adversaries can perform attacks that force victims to use older, more vulnerable versions of software are called downgrade attacks.

Technical Summary

- **Sensitive Exposed Ports:** Each exposed port to the public internet is a front door for the attacker to try and infiltrate. During reconnaissance, certain services were identified that were publicly accessible which may be unused by the application. When legitimate services are exposed to the public internet, these may be exploited through code execution or miss-configurations.
    - **Recommendation:** Opening ports to public internet should be on a "need-to-be" basis. Implement continuous monitoring technologies to identify risks in these open ports.
- **Breached Email Accounts:** Some of the corporate email accounts were found in the database of hacked websites and leaked passwords. This may be serious consequences as the Cyber-Criminals could take control of breached account email account and send fraudulent emails to known contacts and steal their personal and financial information.
    - **Recommendation:** Check and update your computer’s security. Use the latest Endpoint Security software and update its malware database regularly. Further, enforce strong password policies in the corporate network. Use added security features like Multi-Factor authentication to addition login security. Enforce Password-Rotations every two months. Lastly, refrain from clicking on links without validating its legitimacy.
- **Service Information Disclosure:** The HTTP response header(s) disclose information about the installed technologies on the server. This type of issues is non-exploitable in most cases and considered as web application security issues that allow attackers to gather information about the application server which can be used later in the attack lifecycle.
    - **Recommendation:** Configure the technologies such that their headers or messages (success or error) do not disclose information regarding their version and properties.
- **Missing Security headers:** The security headers are fundamental to the development of a web application as these protect against attacks which most websites are vulnerable such as Cross-Site-Scripting (XSS), code injection, click-jacking, etc.
    - **Recommendation:** Enforce the relevant security headers by default, unless there are overriding concerns in which case, such specific headers should be removed or modified.
- **Expired SSL/TLS Certificate:** Certificate seems to have been expired on services of the domain. This puts the personal information of the customers at risk especially when sensitive operations such as financial transaction are carried out. This can also result in decline in sales and revenue as customers do not trust site anymore.

- **Recommendation:** Renew certificate from reputed certificate authorities to ensure trust from the customers.

- **DMARC Missing:** Domain-based Message Authentication, Reporting, and Conformance (DMARC) is a mechanism for policy distribution by which an organization that is the originator of an email ensures that it is protected from phishing, spoofing or fraud attacks. It ensures that legitimate emails are properly authenticated and fraudulent activity which appear to come a domain under the organisation control is blocked before reaching end customer.

  - **Recommendation:** A DMARC policy allows a sender's domain to indicate that their emails are protected by SPF and/or DKIM, and tells a receiver what to do if neither of those authentication methods passes - such as to reject the message or quarantine it. The policy can also specify how an email receiver can report back to the sender's domain about messages that pass and/or fail.

- **Outdated Software:** There are technologies installed on the server which were identified as outdated and have vulnerabilities. If there are known exploits in exploit databases(or deep web) for these vulnerabilities, an attacker may leverage them and gain access to the organisation network.

  - The software hosted on TCP port 587 in host IP Xxxx.xxxx.xxxx.xxxx is running an outdated software Exim smtpd 4.91
  - The software hosted on TCP port 80 in host IP Xxxx.xxxx.xxxx.xxxx is running an outdated software Apache httpd 2.4.25
  - The software hosted on TCP port 443 in host IP Xxxx.xxxx.xxxx.xxxx is running an outdated software Apache httpd 2.4.25
  - The software hosted on TCP port 631 in host IP Xxxx.xxxx.xxxx.xxxx is running an outdated software Apache httpd 2.2.16

    - **Recommendation:** Update the relevant technology to the latest version or install the necessary patch to fix the vulnerability. If there are dependencies on legacy application or libraries, install industry-recommended endpoint security solutions to detect and prevent attacks.

- **SSL/TLS Version:** The target domain uses outdated cypher suites that are often vulnerable to attacks. These protocols may be affected by vulnerabilities such as FREAK, POODLE, BEAST, and CRIME. If you must still support TLS 1.0, disable TLS 1.0 compression to avoid CRIME attacks.

  - **Recommendation:** Use modern cryptographic cypher suites and algorithms with desirable performance and security properties TLS/SSL protocols-based attacks.

Vendor Recommendation

- Please refer to Appendix: Recommendation for more information.

Investigation

This chapter lays out the information gathering that was performed regarding xxxxxx internet-facing infrastructure. More information sources were queried than reported in this chapter; sources that did not yield relevant information were left out.

HTTP Headers

A great deal of information can be gathered in a check of the HTTP Headers from a web server. Server-side software can be identified often down to the exact version running. Cookie strings, web application technologies and other data can be gathered from the HTTP Header. This information can be used when troubleshooting or when planning an attack against the web server.

HTTP Header Info
HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 08:19:36 GMT Server: Apache/2 X-Powered-By: PHP/7.0.32 Link: <http://xxxxxx/wp-json/>; rel="https://api.w.org/", <http://xxxxxxx/wp-json/wp/v2/pages/20>; rel="alternate"; type="application/json", <http://xxxxxxxx/>; rel=shortlink Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Vary: Accept-Encoding,User-Agent Content-Encoding: gzip Content-Length: 8404 Keep-Alive: timeout=2, max=100 Content-Type: text/html; charset=UTF-8

The following information was identified from the web server

- Server (Apache/2)
- X-Powered-By (PHP/7.0.32)

Finding 1: The HTTP response header(s) disclose information on the installed technology. An attacker can use that information to research vulnerabilities in those technologies to attack the application and breach the system.
[Severity of this risk: LOW]

These HTTP responses were inspected to identify the various security header implemented on the web application. These headers prevent modern browsers from running into easily preventable vulnerabilities.

These following security headers were missing from web application response:

- **Strict-Transport-Security**: This header informs the browser that it should never load the website using HTTP and should automatically convert all HTTP request to HTTPS request instead.
- **X-Frame-Options**: Indicates whether the browser should render a page in <frame>, <iframe>, <embed> or <object>. This header can prevent click-jacking attacks by ensuring content is not embedded into other sites.
- **X-Content-Type-Options**: Ensures that marker used to indicate the MIME type of the Content-Type is not allowed to be changed or tampered. This response HTTP headers prevents MIME type sniffing stacks.
- **Content-Security-Policy**: Offers an added layer of protection that help mitigate certain types of attacks, such as Cross Site Scripting (XSS) and data injection attacks. Such attacks are often used for data theft, site defacement and malware distribution.
- **X-Permitted-Cross-Domain-Policies**: Enforces the cross-domain policies which client like Flash and Adobe could use. This is to prevent Flash and Adobe Acrobat from loading content from one's domain from another website which may lead to unexpected data disclosure.

- **Referrer-Policy**: Controls how much referrer information should be included with the request. Flags such as "no-referrer" ensures that no referrer information is sent along a request.
- **Expect-CT**: Allows sites to report or enforce Certificate transparency requirements to prevent the use of miss-issued certificates for that site from going unnoticed.
- **X-XSS-Protection**: Prevents a website from loading when they detect reflected cross-site-scripting attack. Although modern browsers use Content-Security-Policy headers which disables the use of in-line JavaScript, on older browser this header can still provide protection.

Finding 2: The security headers are fundamental to the development of a web application as these protect against attacks which most websites are vulnerable such as Cross-Site-Scripting(XSS), code injection, click-jacking, etc. *[Severity of this risk: MEDIUM]*

Discoverable Links

The section displays the links of the website from all public sources.

Links
http://xxxxxxxx.pl
http://xxxxxxxx.pl
http://xxxxxxxx.pl
http://xxxxxxxx.pl
http://xxxxxxxx.pl
http://xxxxxxxx.pl
http://xxxxxxxx.pl
http://xxxxxxxx.pl

Remark: The severity of disclosed link is best realised by the organisation. The results are included as point of interest. *[Severity: Remark]*

Organisation Email Addresses

The section displays domain specific emails addresses gathered from public sources. Organisational email addresses are often subjected to phishing attacks, which helps an attacker gain foothold in their internal network.

Email Addresses
wxxxxxxx@xxxxxx.pl
mxxxxxxxxxx@ xxxxxx.pl
dxxxxx@ xxxxxx.pl
gxxxxxx@ xxxxxx.pl
gxxxxxxxx@ xxxxxx.pl
txxxxxxxx@ xxxxxx.pl
xxxxxxxxx@ xxxxxx.pl
mxxxxxxx@ xxxxxx.pl
mxxxxxxx@ xxxxxx.pl
wxxxxxxx@ xxxxxx.pl
xxxxxxxx@ xxxxxx.pl
axxxxxxx@ xxxxxx.pl
gxxxxxxx@ xxxxxx.pl
rxxxxxxx@ xxxxxx.pl
wxxxxxxx@ xxxxxx.pl
zxxxxxx@ xxxxxx.pl

The gathered email addresses were further verified by checking against hacked and breached databases. The following was found:

Email Addresses	Breach Database
wxxxxxxx@ xxxxxx.pl	MyHeritage
dxxxxxx@ xxxxxx.pl	Dailymotion
sxxxxxxxx@ xxxxxx.pl	Dailymotion, Dropbox
mxxxxxxx@ xxxxxx.pl	Cit0day
w.xxxxxxx@ xxxxxx.pl	Cit0day, Dailymotion
zxxxxxxxx@ xxxxxx.pl	Cit0day, Dailymotion, MyHeritage
axxxxxxxx@ xxxxxx.pl	AntiPublic
gxxxxxxxxx@ xxxxxx.pl	AntiPublic, Cit0day
rxxxxxxxxx@ xxxxxx.pl	AntiPublic, Cit0day, Collection1

Note that certain sources may be marked as "Sensitive Source". This is because revealing the source may compromise an on-going investigation or the affected site is of a controversial nature.

For more information on the above listed breaches, refer to Appendix B: Known Breaches

It is imperative to understand how the email addresses were compromised. This is likely to happen in few ways:

- The software security in place is not up-to-date.
- A weak password policy is in place, which was easily cracked, or brute forced.
- Vulnerable to social engineering attack. An unsuspecting user may click on a malicious link in an email, IM conversation, or on a social engineering site, or webpage.
- Insufficient security enforcements like password rotation or Multi-Factor Authentications.

Finding 3: Some of the corporate email accounts were found in the database of hacked websites and leaked passwords. This may be serious consequences as the Cyber-Criminals could take control of breached account email account and send fraudulent emails to known contacts and steal their personal and financial information. *[Severity of this risk: MEDIUM]*

Reverse DNS for Subdomain Enumeration

Reverse DNS helps discover the domain name associated with an IP Address by returning its PTR Record. This is one of the common techniques used by attacker to build organisation footprint.

Domain	IP Address
xxxxxx.pl	xxxx.xxxx.xxxx.xxxx
ca10.xxxxxx.pl	xxxx.xxxx.xxxx.xxxx
c1. xxxxxx.pl	xxxx.xxxx.xxxx.xxxx
c2. xxxxxx.pl	xxxx.xxxx.xxxx.xxxx
dns2. xxxxxx.pl	xxxx.xxxx.xxxx.xxxx
ir. xxxxxx.pl	xxxx.xxxx.xxxx.xxxx
c3. xxxxxx.pl	xxxx.xxxx.xxxx.xxxx

DMARC Check

Domain-based Message Authentication, Reporting, and Conformance (DMARC) is a mechanism for policy distribution by which an organization that is the originator of an email ensures that it is protected from phishing, spoofing or fraud attacks. It ensures that legitimate emails are properly authenticated and fraudulent activity which appear to come a domain under the organisation control is blocked before reaching end customer.

No DMARC Record found for Xxxx.

Finding 4: The domain is missing the DMARC authentication mechanism. Without DMARC, the attacker would be able sent fake emails to organisations, and SMTP by default would not have any protection against fake "From" addresses.
[Severity of this risk: HIGH]

A DMARC policy allows a sender's domain to indicate that their emails are protected by SPF and/or DKIM, and tells a receiver what to do if neither of those authentication methods passes - such as to reject the message or quarantine it. The policy can also specify how an email receiver can report back to the sender's domain about messages that pass and/or fail.

Geolocation Information

Eyesight determines the geolocation of the IP addresses asssociated to the organisation. Eyesight attempts to pinpoint which country an IP address is associated with using information from the RIRs (Regional Internal Registries) and other location data.

IP Address	Geolocation
xxxx.xxxx.xxxx.xxxx	xxxxxxxxxxxxxxxxx, Europe
xxxx.xxxx.xxxx.xxxx	xxxxxxxxxxxxxxxxx, Europe
xxxx.xxxx.xxxx.xxxx	xxxxxxxxxxxxxxxxx, Europe
xxxx.xxxx.xxxx.xxxx	xxxxxxxxxxxxxxxxx, Europe
xxxx.xxxx.xxxx.xxxx	xxxxxxxxxxxxxxxxx, Europe
xxxx.xxxx.xxxx.xxxx	xxxxxxxxxxxxxxxxx, Europe
xxxx.xxxx.xxxx.xxxx	xxxxxxxxxxxxxxxxx, Europe
xxxx.xxxx.xxxx.xxxx	xxxxxxxxxxxxxxxxx, Europe
xxxx.xxxx.xxxx.xxxx	xxxxxxxxxxxxxxxxx, Europe
xxxx.xxxx.xxxx.xxxx	xxxxxxxxxxxxxxxxx, Europe
xxxx.xxxx.xxxx.xxxx	xxxxxxxxxxxxxxxxx, Europe
xxxx.xxxx.xxxx.xxxx	xxxxxxxxxxxxxxxxx, Europe
xxxx.xxxx.xxxx.xxxx	xxxxxxxxxxxxxxxxx, Europe
xxxx.xxxx.xxxx.xxxx	xxxxxxxxxxxxxxxxx, Europe
xxxx.xxxx.xxxx.xxxx	xxxxxxxxxxxxxxxxx, Europe
xxxx.xxxx.xxxx.xxxx	xxxxxxxxxxxxxxxxx, Europe
xxxx.xxxx.xxxx.xxxx	xxxxxxxxxxxxxxxxx, Europe
xxxx.xxxx.xxxx.xxxx	xxxxxxxxxxxxxxxxx, Europe
xxxx.xxxx.xxxx.xxxx	xxxxxxxxxxxxxxxxx, Europe
xxxx.xxxx.xxxx.xxxx	xxxxxxxxxxxxxxxxx, Europe
xxxx.xxxx.xxxx.xxxx	xxxxxxxxxxxxxxxxx, Europe
xxxx.xxxx.xxxx.xxxx	xxxxxxxxxxxxxxxxx, Europe
xxxx.xxxx.xxxx.xxxx	xxxxxxxxxxxxxxxxx, Europe

Management Access Advisory From Aruba

In the past few years, there has been an increased focus across the security industry on the risks of exposing internal services to the public Internet. The explosion of the Internet-of-Things trend, with the addition of (frequently insecure) web interfaces to small devices in corporate and home networks, has helped push the risks that exposing internal network services to the Internet can pose into the general consciousness.

Eyesight leverages Shodan search engine to expose insecure Aruba server instances across the Internet. This module guides administrators through the process of limiting access to the management interfaces of the Aruba Access Point, Aruba Controller and Aruba ClearPass products.

This is not an Aruba instance.

Cisco Umbrella Risk Score

The Umbrella Investigate Risk Score is based on an analysis of the lexical characteristics of the domain name and patterns in queries and requests to the domain. It is scaled from 0 to 100, with 100 being the highest risk and 0 being no risk at all. Periodically Umbrella updates this score based on additional inputs. A domain blocked by Umbrella receives a score of 100.

The Cisco Umbrella has classified this domain to be Low Risk.

Malicious Domain Check

Cisco Umbrella keeps a database of all websites that have been known to be malicious and prevents users from accessing the site. The results from the subdomain discovery were further verified against Cisco Umbrella database to identify these malicious domains.

No malicious domains were identified associated with the domain provided.

The Umbrella Investigate integration with Cisco AMP Threat Grid shows samples from the ThreatGrid database associated with a domain, IP or URL that you're looking to find out more information about. Information about samples is provided in the form of checksums associated when looking up a specific host or IP.

Malware Sample Number	1
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
sha256 hash:	7b5782eb288699944d9247003ef12cde58844289617e4e9a5f19a2137175....
Lastseen Date:	2019-09-11 15:28:23
Sample Size:	11983872
Threat Score:	100

Malware Sample Number	2
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
sha256 hash:	3e36dabddfbc80998f29ba82833a4167d4e0b5bcccd242cbf5e841ed3d28....
Lastseen Date:	2019-11-06 01:28:45
Sample Size:	14894080
Threat Score:	100

Malware Sample Number	3
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
sha256 hash:	7a5acafa7c3d72991ed3e9cbceacacd1b5627911831cadb9367f18595be4....
Lastseen Date:	2019-12-13 03:06:08
Sample Size:	15235584
Threat Score:	100

Note that "threat score" given to a particular sample based on the analysis performed by Threat Grid. A threatScore is a measure of the amount of system weakening, obfuscation, persistence, modification, data exfiltration, and other behaviors which may be a threat to the host system's integrity. It is intended as an overall threat indicator that can be used as a guide to the likelihood that a submission is malicious. The Threat Score is not an authoritative classification of good and bad software.

Open Network Ports

Publicly accessible ports increase organisation's security risk especially when these belong to sensitive application on the server. The following section identifies all the open ports/services accessible publicly.

IP Address Xxxx.xxxx.xxxx.xxxx

Port	Version or Response

443	443 HTTP/1.1 200 OK Content-Type: text/html; charset=utf-8 Transfer-Encodin..
22	22 SSH-1.99-Cisco-1.25 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAA.....

IP Address Xxxx.xxxx.xxxx.xxxx

Port	Version or Response
995	995 +OK Dovecot DA ready. +OK CAPA TOP UIDL RESP-CODES PIPELINING AUTH-RESP..
53	53 9.10.3-P4-Debian Resolver name: xxxx.xxxx.pl..
587	587 Exim smtpd 4.91..
25	25 Exim smtpd 4.91..
80	80 Apache httpd 2..
993	993 * OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE LITER..
53	53 9.10.3-P4-Debian Resolver name: xxxx.xxxx.pl..
443	443 Apache httpd 2..
21	21 Pure-FTPd..
143	143 * OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE LITER..
465	465 Exim smtpd 4.91..
2222	2222 HTTP/1.1 200 OK Server: DirectAdmin Daemon v1.60.1 Registered to Naj....

IP Address Xxxx.xxxx.xxxx.xxxx

Port	Version or Response
5222	5222 <stream:stream xmlns='jabber:client' xml:lang='en-US.UTF-8' xmlns:stre..
443	443 cpe:/a:jquery:jquery..
8443	8443 HTTP/1.1 400 Bad Request Date: Fri, 27 Aug 2021 09:21:01 GMT Connectio..

IP Address Xxxx.xxxx.xxxx.xxxx

Port	Version or Response
25	25 Postfix smtpd..
80	80 Apache httpd 2.4.25..
53	53..

IP Address Xxxx.xxxx.xxxx.xxxx

Port	Version or Response
80	80 Apache httpd 2..
21	21 Pure-FTPd..
443	443 Apache httpd 2..

993	993 * OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE LITER..
2222	2222 HTTP/1.1 302 Found Server: DirectAdmin Daemon v1.59.4 Location: https:..
143	143 * OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE LITER..
53	53 9.10.3-P4-Debian Resolver name: xxxx.xxxx.xxxx.pl..
25	25 Exim smtpd..
995	995 +OK Dovecot DA ready. +OK CAPA TOP UIDL RESP-CODES PIPELINING AUTH-RESP..
587	587 Exim smtpd..

IP Address Xxxx.xxxx.xxxx.xxxx

Port	Version or Response
80	80 uc-httpd 1.0.0..
123	123 ntpd "4"..

IP Address Xxxx.xxxx.xxxx.xxxx

Port	Version or Response
21	21 Pure-FTPd..

IP Address Xxxx.xxxx.xxxx.xxxx

Port	Version or Response
443	443 Apache httpd 2.4.25..
21	21 ProFTPD 1.3.5b..

IP Address Xxxx.xxxx.xxxx.xxxx

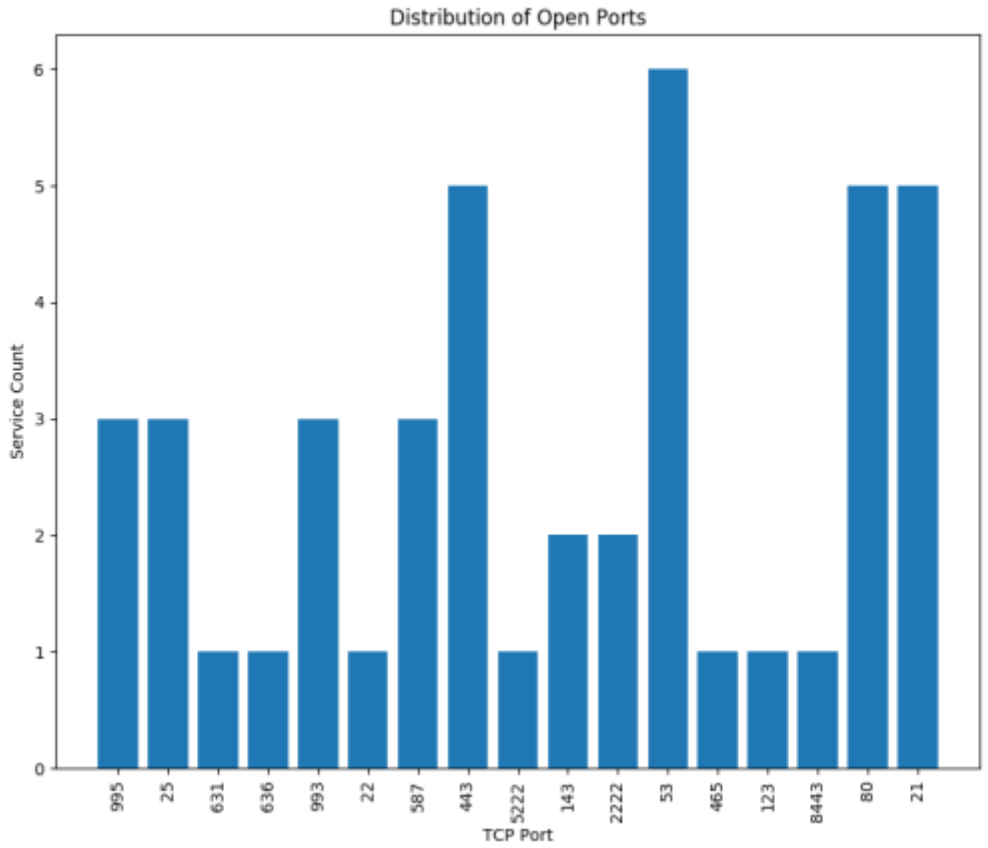
Port	Version or Response
631	631 Apache httpd 2.2.16..
80	80 Apache httpd 2.2.16..
21	21 Pure-FTPd..
636	636 HTTP/1.1 404 Not Found Date: Sat, 18 Sep 2021 05:08:34 GMT Server: Apac..
587	587 Postfix smtpd..
993	993 * OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE A..
53	53..
995	995 +OK Dovecot ready. +OK CAPA TOP UIDL RESP-CODES PIPELINING USER SASL PL..

53	53..

Sensitive Ports (Exposed)

The open ports can be dangerous when the service listening on the port is misconfigured, unpatched, vulnerable to exploits, or has poorly configured security rules. The following section describes the security risks produces by some of the above disclosed open TCP ports.

The following graph demonstrates the open TCP ports across the target domain and its subdomains:



The detailed list of publicly accessible services in the domain is below:

DNS (Domain Name System)	PORT: 53
Risk	If DNS service is poorly secured, this can cause widespread disruption with attacks such as a distributed denial of service(DDoS) where the attacker targets the DNS Servers. This service is often used by attackers as an exit strategy where confidential data is smuggled outside the network via DNS tunnelling
Recommendation	Patch DNS servers regularly to minimise vulnerabilities. Inspect the traffic to/from port 53 to prevent data exfiltration.

SSH (Secure Shell)	PORT: 22
Risk	A web service need not have a publicly accessible SSH service. This allows an attacker to guess or brute-force credentials and gain access to the server.
Recommendation	Disable the service if access is not mandatory. If public access is required, use a VPN to access via the internal network. Enable and configure firewalls to filter the incoming traffic to the service.

SMTP (Simple Mail Transfer Protocol)	PORT: 25
Risk	If the service is not monitored or configured, spammers can connect to the target server and send unsolicited emails.
Recommendation	Specify trusted sources which can connect into your network on this Port using a firewall or the mail server. On an Exchange server, this can be achieved by creating a Receive Connector and only allowing it to accept SMTP traffic from designated IP's.

FTP (File Transfer Protocol)	PORT: 21
Risk	FTP is often considered as an insecure protocol as data is sent in clear text format and offers an anonymous option with no password request.
Recommendation	Ensure that access to the service is password protected and anonymous login is disabled. Furthermore, enforce IP white-list on the service thereby allowing only limited access to the port.

Finding 5: Each exposed port to the public internet is a front door for the attacker to try and infiltrate. During reconnaissance certain services were identified that were publicly accessible which may be unused by the application. When legitimate services are exposed to public internet, these may be exploited through code execution or miss-configurations.

[Severity of this risk: LOW]

Vulnerable Services

The open ports discovered from the previous sections are analysed for vulnerabilities using IOT search engine "Shodan". It allows the security experts to easily locate poorly protected devices exposed over the internet. At the same time, it represents a privileged instrument for the hackers that have to search for a specific target and need to gather information on its configuration.

The following outdated software(s) were discovered:

- The software hosted on TCP port **587** in host IP Xxxx.xxxx.xxxx.xxxx is running an outdated software **Exim smtpd 4.91**
- The software hosted on TCP port **80** in host IP Xxxx.xxxx.xxxx.xxxx is running an outdated software **Apache httpd 2.4.25**
- The software hosted on TCP port **443** in host IP Xxxx.xxxx.xxxx.xxxx is running an outdated software **Apache httpd 2.4.25**

- The software hosted on TCP port **631** in host IP Xxxx.xxxx.xxxx.xxxx is running an outdated software **Apache httpd 2.2.16**

Refer to "Appendix: CVE (Outdated Software)" section for more information on the impacting vulnerabilities.

Finding 6: There are technologies installed on the server which are outdated and are having vulnerabilities. If there are known exploits in exploit databases(or deep web) for these vulnerabilities, an attacker may leverage these and gain access to the organisation network.
[Severity of this risk: HIGH]

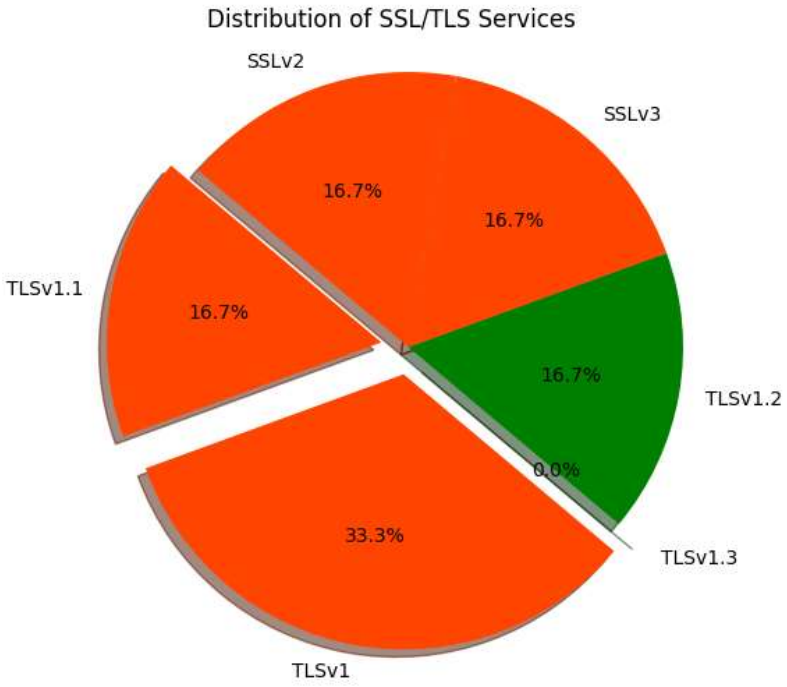
SSL/TLS Information

When a user connects to a web site with HTTPS, the application server returns a list of ciphers to encrypt the data stream. If weak ciphers were offered, secure communications can easily be defeated by a skilled attacker. Furthermore, the SSL certificates are used to create an encrypted channel between the client and the server. They are means to offer trust to the end user and an assurance that they are communicating with the indented party.

The services employing SSL/TLS are investigated further and following information was gathered:

Service	443 (https) (Xxxx.xxxx.xxxx.xxxx)
Accepted SSL/TLS Protocols	TLSv1 TLSv1.1 TLSv1.2
Certificate Signature Algorithm	sha1WithRSAEncryption (Bits: 1024, Type: rsa)
Is Certificate Expired:	False
Service	587 (smtp) (185.216.182.230)
Accepted SSL/TLS Protocols	TLSv1 SSLv2 SSLv3
Certificate Signature Algorithm	sha1WithRSAEncryption (Bits: 1024, Type: rsa)
Is Certificate Expired:	True

The following graph demonstrates the services using SSL/TLS protocols across the target domain and its subdomains:



Outdated SSL/TLS Protocols

On March of 2020, Firefox and other popular browsers disabled the support of TLS 1.1 along with TLS 1.0. As these protocols do not support modern cryptographic algorithms, their existence on the application server remains a security risk.

The employment of the latest TLS version such TLS1.2 and higher, come with many benefits:

- These have desirable performance and security properties, such as perfect forward secrecy and authenticated encryption.
- As part of peer authentication, mandatory and insecure SHA-1 and MD5 hash functions were removed.
- Resistance to downgrade-related attacks such as FREAK.

The following services use outdated SSL/TLS ciphers:

- TCP PORT: 587 (Xxxx.xxxx.xxxx.xxxx)
- TCP PORT: 443 (Xxxx.xxxx.xxxx.xxxx)

Finding 7: TLS scans identified the domain xxxxxxxx to use outdated cipher suites that are often vulnerable to attacks. These protocols may be affected by vulnerabilities such as FREAK, POODLE, BEAST, and CRIME. If supporting TLS 1.0 is a business requirement, disable TLS 1.0 compression to avoid CRIME attacks. *[Severity of this risk: LOW]*

Expired Security Certificates

Security Certificate expire after a certain validity period and this is means to provide assurance to the security of SSL. The validity period regulates and confirms the authenticity of the server to the web browsers. Among the gathered domain related hosts, the security certificate of the following services were found expired:

- TLS Certificate of the service hosted on TCP PORT 587 (Xxxx.xxxx.xxxx.xxxx) has expired.

Finding 8: Certificate seems to have been expired on services of the domain xxxxxxxx. This puts the personal information of the customers at risk especially when sensitive operations such as financial transaction are carried out. This can also results in decline in sales and revenue as customers do not trust site any more.*[Severity of this risk: MEDIUM]*

Appendix: Additional Gathered intelligence

The following sections describes the various tests conducted on the domain(s).

DNS Lookup

Below are the DNS records for a domain determined using the dig DNS tool.

Record	Value
A	xxxx.xxxx.xxxx.xxxx
MX	xxxxxxx.outlook.com.
NS	ns2.xxxxxxxxxx.pl.
NS	ns1.xxxxxxxxxx.pl.
TXT	"ciscocidomainverification=asadadd0234aec915156b862c0539d4591d48b3c733270002....."
TXT	"v=spf1 a mx ptr ip4
TXT	"MS=0E1135TR65E4D155B4577A6E"
SOA	dns.xxxxxxx.pl. root.xxxxxxx.pl. 20212342700 2400 3700 1469600 00000

WHOIS Lookup

WHOIS database provides information on domain registration and availability.

WHOIS Result
request limit exceeded

Domain Subnets

The section lists the subnet ranges of the organisation(s) from public sources like ipv4list.info and several others.

IP Info
Address = xxxx.xxxx.xxxx.xxxx Network = xxxx.xxxx.xxxx.xxxx / 32 Netmask = 255.255.255.255 Broadcast = not needed on Point-to-Point links Wildcard Mask = 0.0.0.0 Hosts Bits = 0 Max. Hosts = 1 (2^0 - 0) Host Range = { xxxx.xxxx.xxxx.xxxx - xxxx.xxxx.xxxx.xxxx }

Reverse IP Lookup

Reverse IP lookup lets identifies the websites hosted on a server.

Domain List
axxxxxxxx.pl rxxxxxxxx.pl yxxxxxxxx.pl rxxxxxxxx.pl wxxxxxxxx.pl xxxxxxxxx.pl nxxxxxxxxx.pl xxxxxxxxx.pl sxxxxxxxxx.pl

If there is a security breach on any of the hosted websites, all other websites sharing this host may also be impacted. This setup does not offer any protection even if these websites are running the latest software and protected by WAF.
[Severity : Remark]

Appendix: Known Breaches

Breach Name	Description
AntiPublic	In December 2016, a huge list of email address and password pairs appeared in a combo list referred to as Anti Public . The list contained 458 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for credential stuffing , that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read Password reuse, credential stuffing and another billion records in Have I Been Pwned.
Dailymotion	In October 2016, the video sharing platform Dailymotion suffered a data breach. The attack led to the exposure of more than 85 million user accounts and included email addresses, usernames and bcrypt hashes of passwords.
VerificationsIO	In February 2019, the email address validation service verifications.io suffered a data breach. Discovered by Bob Diachenko and Vinny Troia, the breach was due to the data being stored in a MongoDB instance left publicly facing without a password and resulted in 763 million unique email addresses being exposed. Many records within the data also included additional personal attributes such as names, phone numbers, IP addresses, dates of birth and genders. No passwords were included in the data. The Verifications.io website went offline during the disclosure process, although an archived copy remains viewable.
Adobe	In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, encrypted password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.
ExploitIn	In late 2016, a huge list of email address and password pairs appeared in a combo list referred to as Exploit.In . The list contained 593 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for credential stuffing , that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read Password reuse, credential stuffing and another billion records in Have I Been Pwned.

Autocentrum	In February 2018, data belonging to the Polish motoring website autocentrum.pl was found online. The data contained 144k email addresses and plain text passwords.
2844Breaches	In February 2018, a massive collection of almost 3,000 alleged data breaches was found online. Whilst some of the data had previously been seen in Have I Been Pwned, 2,844 of the files consisting of more than 80 million unique email addresses had not previously been seen. Each file contained both an email address and plain text password and were consequently loaded as a single unverified data breach.
Collection1	In January 2019, a large collection of credential stuffing lists (combinations of email addresses and passwords used to hijack accounts on other services) was discovered being distributed on a popular hacking forum. The data contained almost 2.7 billion records including 773 million unique email addresses alongside passwords those addresses had used on other breached services. Full details on the incident and how to search the breached passwords are provided in the blog post The 773 Million Record "Collection #1" Data Breach.
MyHeritage	In October 2017, the genealogy website MyHeritage suffered a data breach. The incident was reported 7 months later after a security researcher discovered the data and contacted MyHeritage. In total, more than 92M customer records were exposed and included email addresses and salted SHA-1 password hashes. In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it be attributed to BenjaminBlue@exploit.im .
Dropbox	In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).
Cit0day	In November 2020, a collection of more than 23,000 allegedly breached websites known as Cit0day were made available for download on several hacking forums. The data consisted of 226M unique email address alongside password pairs, often represented as both password hashes and the cracked, plain text versions. Independent verification of the data established it contains

many legitimate, previously undisclosed breaches. The data was provided to HIBP by dehashed.com.

Appendix: CVE (Outdated Software)

The vulnerabilities impacting the software Exim smtpd 4.91 on TCP port (587)(xxxx.xxxx.xxxx.xxxx)

Note that the host/device may not be impacted by all of these issues mentioned below. The vulnerabilities are implied based on the software and version.

CVE	CVSS	Verified	Summary
CVE-2019-13917	10.0	False	Exim 4.85 through 4.92 (fixed in 4.92.1) allows remote code execution as root in some unusual configurations that use the ${sort } expansion for items that can be controlled by an attacker (e.g., $local_part or $domain).
CVE-2019-10149	7.5	False	A flaw was found in Exim versions 4.87 to 4.91 (inclusive). Improper validation of recipient address in deliver_message() function in /src/deliver.c may lead to remote command execution.

The vulnerabilities impacting the software Apache httpd 2.4.25 on TCP port (80)(xxxx.xxxx.xxxx.xxxx)

Note that the host/device may not be impacted by all of these issues mentioned below. The vulnerabilities are implied based on the software and version.

CVE	CVSS	Verified	Summary
CVE-2019-0220	5.0	False	A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.
CVE-2018-1333	5.0	False	By specially crafting HTTP/2 requests, workers would be allocated 60 seconds longer than necessary, leading to worker exhaustion and a denial of service. Fixed in Apache

			HTTP Server 2.4.34 (Affected 2.4.18-2.4.30,2.4.33).
CVE-2020-1927	5.8	False	In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.
CVE-2019-10098	5.8	False	In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.
CVE-2019-0197	4.9	False	A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38. When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. Server that never enabled the h2 protocol or that only enabled it for https: and did not set "H2Upgrade on" are unaffected by this issue.
CVE-2019-0196	5.0	False	A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.
CVE-2017-7659	5.0	False	A maliciously constructed HTTP/2 request could cause mod_http2 in Apache HTTP Server 2.4.24, 2.4.25 to dereference a NULL pointer and crash the server process.
CVE-2017-9788	6.4	False	In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between

			successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.
CVE-2017-9798	5.0	False	Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.
CVE-2019-0211	7.2	False	In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.
CVE-2017-15710	5.0	False	In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right

			charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.
CVE-2018-11763	4.3	False	In Apache HTTP Server 2.4.17 to 2.4.34, by sending continuous, large SETTINGS frames a client can occupy a connection, server thread and CPU time without any connection timeout coming to effect. This affects only HTTP/2 connections. A possible mitigation is to not enable the h2 protocol.
CVE-2018-1283	3.5	False	In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to forward its session data to CGI applications (SessionEnv on, not the default), a remote user may influence their content by using a "Session" header. This comes from the "HTTP_SESSION" variable name used by mod_session to forward its data to CGIs, since the prefix "HTTP_" is also used by the Apache HTTP Server to pass HTTP header fields, per CGI specifications.
CVE-2017-3167	7.5	False	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may

			lead to authentication requirements being bypassed.
CVE-2018-1312	6.8	False	In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.
CVE-2017-7668	7.5	False	The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allows ap_find_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap_find_token() to return an incorrect value.
CVE-2017-3169	7.5	False	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.
CVE-2018-17199	5.0	False	In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.
CVE-2017-7679	7.5	False	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.
CVE-2017-15715	6.8	False	In Apache httpd 2.4.0 to 2.4.29, the expression specified in <FilesMatch> could

			match '$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are are externally blocked, but only by matching the trailing portion of the filename.

The vulnerabilities impacting the software Apache httpd 2.4.25 on TCP port (443)(xxxx.xxxx.xxxx.xxxx)

Note that the host/device may not be impacted by all of these issues mentioned below. The vulnerabilities are implied based on the software and version.

CVE	CVSS	Verified	Summary
CVE-2019-0220	5.0	False	A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.
CVE-2018-1333	5.0	False	By specially crafting HTTP/2 requests, workers would be allocated 60 seconds longer than necessary, leading to worker exhaustion and a denial of service. Fixed in Apache HTTP Server 2.4.34 (Affected 2.4.18-2.4.30,2.4.33).
CVE-2020-1927	5.8	False	In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.
CVE-2019-10098	5.8	False	In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.

CVE-2019-0197	4.9	False	A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38. When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. Server that never enabled the h2 protocol or that only enabled it for https: and did not set "H2Upgrade on" are unaffected by this issue.
CVE-2019-0196	5.0	False	A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.
CVE-2017-7659	5.0	False	A maliciously constructed HTTP/2 request could cause mod_http2 in Apache HTTP Server 2.4.24, 2.4.25 to dereference a NULL pointer and crash the server process.
CVE-2017-9788	6.4	False	In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.
CVE-2017-9798	5.0	False	Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain

			misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.
CVE-2019-0211	7.2	False	In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.
CVE-2017-15710	5.0	False	In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more

			likely case, this memory is already reserved for future use and the issue has no effect at all.
CVE-2018-11763	4.3	False	In Apache HTTP Server 2.4.17 to 2.4.34, by sending continuous, large SETTINGS frames a client can occupy a connection, server thread and CPU time without any connection timeout coming to effect. This affects only HTTP/2 connections. A possible mitigation is to not enable the h2 protocol.
CVE-2018-1283	3.5	False	In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to forward its session data to CGI applications (SessionEnv on, not the default), a remote user may influence their content by using a "Session" header. This comes from the "HTTP_SESSION" variable name used by mod_session to forward its data to CGIs, since the prefix "HTTP_" is also used by the Apache HTTP Server to pass HTTP header fields, per CGI specifications.
CVE-2017-3167	7.5	False	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.
CVE-2018-1312	6.8	False	In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.
CVE-2017-7668	7.5	False	The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24

			introduced a bug in token list parsing, which allows ap_find_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap_find_token() to return an incorrect value.
CVE-2017-3169	7.5	False	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.
CVE-2018-17199	5.0	False	In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.
CVE-2017-7679	7.5	False	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.
CVE-2017-15715	6.8	False	In Apache httpd 2.4.0 to 2.4.29, the expression specified in <FilesMatch> could match '$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are are externally blocked, but only by matching the trailing portion of the filename.

The vulnerabilities impacting the software Apache httpd 2.2.16 on TCP port (631)(xxxx.xxxx.xxxx.xxxx)

Note that the host/device may not be impacted by all of these issues mentioned below. The vulnerabilities are implied based on the software and version.

CVE	CVSS	Verified	Summary

CVE-2011-4317	4.3	False	The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an @ (at sign) character and a : (colon) character in invalid positions. NOTE: this vulnerability exists because of an incomplete fix for CVE-2011-3368.
CVE-2017-7679	7.5	False	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.
CVE-2018-1312	6.8	False	In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.
CVE-2011-3368	5.0	False	The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21 does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an initial @ (at sign) character.
CVE-2011-3348	4.3	False	The mod_proxy_ajp module in the Apache HTTP Server before

			2.2.21, when used with mod_proxy_balancer in certain configurations, allows remote attackers to cause a denial of service (temporary "error state" in the backend server) via a malformed HTTP request.
CVE-2012-3499	4.3	False	Multiple cross-site scripting (XSS) vulnerabilities in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via vectors involving hostnames and URIs in the (1) mod_imagemap, (2) mod_info, (3) mod_ldap, (4) mod_proxy_ftp, and (5) mod_status modules.
CVE-2012-4558	4.3	False	Multiple cross-site scripting (XSS) vulnerabilities in the balancer_handler function in the manager interface in mod_proxy_balancer.c in the mod_proxy_balancer module in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via a crafted string.
CVE-2013-1896	4.3	False	mod_dav.c in the Apache HTTP Server before 2.2.25 does not properly determine whether DAV is enabled for a URI, which allows remote attackers to cause a denial of service (segmentation fault) via a MERGE request in which the URI is configured for handling by the mod_dav_svn module, but a certain href attribute in XML data refers to a non-DAV URI.
CVE-2016-8612	3.3	False	Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process.
CVE-2016-4975	4.3	False	Possible CRLF injection allowing HTTP response splitting attacks for sites which

			use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).
CVE-2012-4557	5.0	False	The mod_proxy_ajp module in the Apache HTTP Server 2.2.12 through 2.2.21 places a worker node into an error state upon detection of a long request-processing time, which allows remote attackers to cause a denial of service (worker consumption) via an expensive request.
CVE-2017-7668	7.5	False	The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allows ap_find_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap_find_token() to return an incorrect value.
CVE-2013-6438	5.0	False	The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.
CVE-2012-2687	2.6	False	Multiple cross-site scripting (XSS) vulnerabilities in the make_variant_list function in mod_negotiation.c in the mod_negotiation module in the Apache HTTP Server 2.4.x before 2.4.3, when the MultiViews option is enabled, allow remote attackers to inject arbitrary web script or

			HTML via a crafted filename that is not properly handled during construction of a variant list.
CVE-2011-4415	1.2	False	The ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, does not restrict the size of values of environment variables, which allows local users to cause a denial of service (memory consumption or NULL pointer dereference) via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, related to (1) the "len +=" statement and (2) the apr_pcalloc function call, a different vulnerability than CVE-2011-3607.
CVE-2012-0031	4.6	False	scoreboard.c in the Apache HTTP Server 2.2.21 and earlier might allow local users to cause a denial of service (daemon crash during shutdown) or possibly have unspecified other impact by modifying a certain type field within a scoreboard shared memory segment, leading to an invalid call to the free function.
CVE-2013-2249	7.5	False	mod_session_dbd.c in the mod_session_dbd module in the Apache HTTP Server before 2.4.5 proceeds with save operations for a session without considering the dirty flag and the requirement for a new session ID, which has unspecified impact and remote attack vectors.
CVE-2011-3607	4.4	False	Integer overflow in the ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, allows local users to gain privileges via a .htaccess file with a crafted

			SetEnvIf directive, in conjunction with a crafted HTTP request header, leading to a heap-based buffer overflow.
CVE-2017-3167	7.5	False	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.
CVE-2012-0053	4.3	False	protocol.c in the Apache HTTP Server 2.2.x through 2.2.21 does not properly restrict header information during construction of Bad Request (aka 400) error documents, which allows remote attackers to obtain the values of HTTPOnly cookies via vectors involving a (1) long or (2) malformed header in conjunction with crafted web script.
CVE-2012-0883	6.9	False	envvars (aka envvars-std) in the Apache HTTP Server before 2.4.2 places a zero-length directory name in the LD_LIBRARY_PATH, which allows local users to gain privileges via a Trojan horse DSO in the current working directory during execution of apachectl.
CVE-2017-3169	7.5	False	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.
CVE-2011-3639	4.3	False	The mod_proxy module in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x before 2.2.18, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows

			remote attackers to send requests to intranet servers by using the HTTP/0.9 protocol with a malformed URI containing an initial @ (at sign) character. NOTE: this vulnerability exists because of an incomplete fix for CVE-2011-3368.
CVE-2011-0419	4.3	False	Stack consumption vulnerability in the fnmatch implementation in apr_fnmatch.c in the Apache Portable Runtime (APR) library before 1.4.3 and the Apache HTTP Server before 2.2.18, and in fnmatch.c in libc in NetBSD 5.1, OpenBSD 4.8, FreeBSD, Apple Mac OS X 10.6, Oracle Solaris 10, and Android, allows context-dependent attackers to cause a denial of service (CPU and memory consumption) via *? sequences in the first argument, as demonstrated by attacks against mod_autoindex in httpd.
CVE-2014-0231	5.0	False	The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.
CVE-2013-1862	5.1	False	mod_rewrite.c in the mod_rewrite module in the Apache HTTP Server 2.2.x before 2.2.25 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to execute arbitrary commands via an HTTP request containing an escape sequence for a terminal emulator.
CVE-2014-0098	5.0	False	The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and

			daemon crash) via a crafted cookie that is not properly handled during truncation.
CVE-2011-3192	7.8	False	The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086.

Appendix: Recommendations

The five Functions of the NIST Framework for Cybersecurity (Identify, Protect, Detect, Respond & Recover) were selected because they represent the five primary pillars for a successful and holistic cybersecurity program. They aid organizations in easily expressing their management of cybersecurity risk at a high level and enabling risk management decisions.

HTTP Headers

HTTP header Information disclosure can be used for zero-day attacks/XSS.

NIST Identify	Web Application Testing	Testing the security of web applications and web services
NIST Protect	Web Application Firewall	Web Application Firewall (WAF) - Monitor's web traffic and protects web applications against OWASP Top 10 and other Web Layer Attacks based on Policy, Signature and Learning.

E-Mail and breached databases

Leaked internal information were found. This means either someone has stolen your data and uploaded them somewhere or that your email credentials were listed in a public list. To avoid a breach like this you must first identify the source by ensuring continues execution of Vulnerability Assessments and Penetration Test (VAPT). In addition to that you should provide your employees awareness trainings by installing a phishing protection/simulation. A solution like Data Leak Prevention (DLP) would prevent your users to post sensitive information to the public. To keep attackers out of your infrastructure even if they have your (stolen) user credentials you need to have an Multi Factor Authentication (MFA) in place.

NIST Identify	Vulnerability Assessment	Vulnerability Assessment (VA) - Provides deep insight into an organization's current state of security, and the effectiveness of its countermeasures. Perform Vulnerability Assessment scans, possibly monthly. This will help you to avoid any breach that can cause both financial and/or reputational loss and to evaluate security posture and business exposure.
NIST Identify	Penetration Test	A penetration test (PT), colloquially known as a pen test, pentest or ethical hacking, is an authorized simulated cyberattack on a computer system, performed to evaluate the security of the system
NIST Protect	Phishing Protection	Web Application Firewall (WAF) - Monitor's web traffic and protects web applications against OWASP Top 10 and other Web Layer Attacks based on Policy, Signature and Learning.
NIST Protect	Multi-Factor Authentication	Method of confirming users' claimed identities by using a combination of two or more factors: 1. Something you know, 2. Something you have, 3. Something you are. Enforce multi-factor authentication mechanisms such as a one-time password (OTP) sent to the registered mobile phone, or an OTP generated with a previously issued secure token.
NIST Protect	Data Leak Prevention (DLP)	Data Leakage Prevention (DLP) - Refers to different processes, techniques and solutions that detect and prevent theft of sensitive data and unauthorized data exfiltration.
NIST Protect	Email encryption	Email Encryption encrypts email messages to protect content from being read by entities other than the intended recipients.
NIST Protect	Email Security	Email Security provides collective measures to secure the content of an email account or service. It also allows an individual or organization to protect the overall access to one or more email addresses/accounts.

DNS

The DNS findings in EYESIGHT are just an informational listing. However, scaling and securing every environment helps protect your business from site outages and improves DNS and application performance. Securing DNS infrastructures from the latest DDoS attacks and protecting DNS query responses from cache poisoning helps keep your business online and viable. Discuss the implementation of Domain Name System Security Extensions (DNSSEC) which is a set of specifications that extend the DNS protocol by adding cryptographic authentication for responses received from authoritative DNS servers. Its goal is to defend against techniques that hackers use to direct computers to rogue websites and servers.

NIST Protect	Cloud Workload Protection Platforms (CWPP)	Cloud Workload Protection Platforms (CWPP) - A suite of technology solutions aimed at securing server workloads in public cloud Infrastructure as a Service (IaaS) environments.
NIST Protect	Cross Domain Solution (CDS)	Cross Domain Solution (CDS) - An information assurance measure that governs access to or transfer of information between two or more differing security domains.

SSL/TLS(Certificate) Information

Eyesight lists SSL/TLS certificates incl. Its version, encryption algorithms, service using the certificate and even it shows if they are outdated and be used for a further attack.

NIST Protect	Firewall	Firewall - Network security device that monitors traffic to or from your network. It allows or blocks traffic based on a defined set of security rules.
NIST Protect	Key Management	Key Management System (KMS) - Key management is the process of administering or managing cryptographic keys for a cryptosystem. It involves the generation, creation, protection, storage, exchange, replacement and use of said keys and with another type of security system built into large cryptosystems, enables selective restriction for certain keys.
NIST Protect	Web Application Firewall (WAF)	Web Application Firewall (WAF) - Monitor's web traffic and protects web applications against OWASP Top 10 and other Web Layer Attacks based on Policy, Signature and Learning.
NIST Detect	SSL Visibility	SSL Visibility - Solutions that decrypt encrypted traffic and forwards it to security solutions to detect and prevent threats to the organization.

Open Network Ports

Eyesight lists all Open Network ports on Public IPs: It provides information like port status, running services and its details.

NIST Identify	Vulnerability Assessment	Vulnerability Assessment (VA) - Provides deep insight into an organization's current state of security, and the effectiveness of its countermeasures. Perform Vulnerability Assessment scans, possibly monthly. This will help you to avoid any breach that can cause both financial and/or reputational loss and to evaluate security posture and business exposure.
NIST Identify	Penetration Test	A penetration test (PT), colloquially known as a pen test, pentest or ethical hacking, is an authorized simulated cyberattack on a computer system, performed to evaluate the security of the system
NIST Protect	DDOS	DDOS - provides advanced DDoS prevention, protection and IoT botnet attack mitigation across legacy data center and public cloud.

NIST Protect	Network IPS	Network IPS – Continuously monitors network traffic, looking for possible malicious actors, anomalies, and events, and preventing them from entering protected portions of your organizational network. And it could prevent the external scanning.
NIST Detect	Remote Access VPN	Remote Access VPN - Allows individual users to securely connect and interact with a private network from a remote location using a laptop or desktop computer connected to the internet, instead of having public open ports.

Outdated Software

Eyesight lists all Open Network ports on Public IPs: It provides information like port status, running services and its details.

NIST Identify	Vulnerability Assessment	Vulnerability Assessment - Provides deep insight into an organization's current state of security, and the effectiveness of its countermeasures. Perform Vulnerability Assessment scans, possibly monthly. This will help you to avoid any breach that can cause both financial and/or reputational loss and to evaluate security posture and business exposure.
NIST Protect	Network Intrusion Prevention System (IPS)	A Network IPS continuously monitors network traffic, looking for possible malicious actors, anomalies, and events, and preventing them from entering protected portions of your organizational network.
NIST Protect	Patch Management	Implement a patch management solution and a formal process to acquire, prioritize, test and install applicable patches (code changes) on existing applications and tools in the organizational environment, is enabling systems to stay protected against the latest threats.

Malicious Domain Check

Eyesight checks if malicious code was listed or linked on the provided domain. This can be an indicator of a successful attack. And you should check with the following set of solutions / services if the environment is already breached.

NIST Identify	Vulnerability Assessment	Vulnerability Assessment (VA) - Provides deep insight into an organization's current state of security, and the effectiveness of its countermeasures. Perform Vulnerability Assessment scans, possibly monthly. This will help you to avoid any breach that can cause both financial and/or reputational loss and to evaluate security posture and business exposure.
NIST Identify	Penetration Test	A penetration test (PT), colloquially known as a pen test, pentest or ethical hacking, is an authorized simulated cyberattack on a computer system, performed to evaluate the security of the system
NIST Detect	Security Information and Event Management (SIEM)	Security Information and Event Management (SIEM) - Provide real-time analysis of security alerts generated by applications and network hardware.
NIST Protect	NGFW (Application Control)	Improve security and meet compliance with easy enforcement of your acceptable use policy through unmatched, real-time visibility into the applications your users are running. With Application Control, you can quickly create policies to allow, deny, or restrict access to applications or entire categories of applications.

NIST Protect	Advanced Threat Protection (ATP)	Advanced threat protection (ATP) refers to a category of security solutions that defend against sophisticated malware or hacking-based attacks targeting sensitive data. Advanced threat protection solutions can be available as software or as managed services. ATP solutions can differ in approaches and components, but most include some combination of endpoint agents, network devices, email gateways, malware protection systems, and a centralized management console to correlate alerts and manage defenses.
NIST Protect	Web Application Firewall	Web Application Firewall (WAF) - Monitor's web traffic and protects web applications against OWASP Top 10 and other Web Layer Attacks based on Policy, Signature and Learning.
NIST Protect	Endpoint Detection and Response (EDR) / Endpoint Forensics	End-point Detection and Response (EDR) / End-point Forensics - Refers to techniques and solutions that are used to detect and respond to Advanced Persistent Threats that can evade traditional detection and prevention mechanisms.
NIST Protect	Threat Hunting Services	Threat Hunting - This is a proactive defense strategy to detect threats within the organization that can evade existing security solutions before they become an attack.
NIST Protect	Threat Intelligence	Information an organization uses to understand the threats that have, will, or are currently targeting the organization. This information is used to identify, prepare for and prevent cyber threats targeting valuable resources.

Geolocation

Eyesight shows you the geolocation of the target domains. This could lead to SD-WAN solutions. SD-WAN delivers advanced routing, self-healing capabilities, and flexible security using network firewall or SASE-based cloud-delivered services—all in a single, integrated solution.

NIST Protect	Cloud Security (SASE)	Secure Access Service Edge is a term coined by analyst firm Gartner, SASE simplifies wide-area networking and security by delivering both as a cloud service directly to the source of connection rather than the enterprise data center.
NIST Protect	Cross Domain Solution (CDS)	Cross Domain Solution (CDS) - An information assurance measure that governs access to or transfer of information between two or more differing security domains.

DMARC

Domain-Based Message Authentication, Reporting and Conformance Solutions, better known as DMARC solutions, are a technology which makes email communication safer.

Email is extremely insecure, and it can be difficult to tell whether an email has come a valid sender address or domain. For example, a hacker can exploit Outlook to use the exact same email address a bank would use but be on a completely different domain entirely. DMARC is an authentication service which authenticates email domains to stop this exact situation.

DMARC is a policy layer for email which helps to ensure that emails meet two standards: Domain Keys Identified Mail (DKIM) and Sender-Policy Framework (SPF). These standards help to make sure that emails are not phishing attacks and that emails sent from your domain are compliant with DMARC regulations, so that they are not flagged as being fraudulent or unsafe email communications.

NIST Protect	Email Security	DMARC tools in this category scan all emails to ensure that emails coming in and out of an email network meet SPF and DKIM standards, integrate with tools like a Secure Email Gateway to block email attacks and help to stop phishing emails that are not DMARC compliant from entering an email network.

xxxxxxx

INGRAM MICRO®

SECURITY

Ingram Micro B.V - Papendorpseweg 95 - 3528 BJ Utrecht – The Netherlands