VONAHI SECURITY

Sep 2024 Pen Test

CONSOLIDATED REPORT

Mobly

September 16, 2024

WWW.VONAHI.IO

Copyright

The methodology used to audit the computer systems is considered proprietary intellectual information of Vonahi Security and may not be disclosed without written permission from Vonahi Security. Vonahi Security gives permission to copy this report for the purpose of disseminating information within your organization, or any regulatory agency.

Confidentiality

This document contains company confidential information of a proprietary and sensitive nature. As such, this document should be afforded the security and handling precautions that a confidential document warrants. This document should have a controlled distribution to relevant parties only and should not be copied without written permission. Vonahi Security treats the contents of a security audit as company confidential material and will not disclose the contents of this document to anyone without written permission.

Assessment Project Team

Below is a list of contacts that were involved in this engagement. Should you have any questions pertaining to the content of this document or any project and non-project-related items, please feel free to reach out to the necessary project contacts.

Primary Point of Contact	
Name:	vPenTest Support
Title:	Support
Office:	
Email:	support@vpentest.io

Executive Summary

Mobly has requested the assistance of Vonahi Security to perform a comprehensive security assessment to assist with evaluating the cyber risks presented within the tested environment(s). The objective of this engagement was to determine if any identified threats could be used to mount an attack against the organization that could lead to the disclosure of sensitive information or access to critical information systems.

Included in this Executive Summary report is a high-level overview of the results that were observed during this assessment. A copy of more specific information pertaining to technical findings and remediation details are documented within the Technical Report as well as the Vulnerability Tracking Report.

Engagement Scope of Work

Prior to beginning the assessment, Vonahi Security and Mobly agreed to a scope of work to define the specific assessment phases. The table below outlines the engagement scope of work and details entailed within each assessment phase that was conducted as part of this engagement.

Assessment Component	Assessment Phases
External Network Security Assessment	During this phase, Open Source Intelligence (OSINT) Gathering is researched to identify valuable information that may contribute to a successful attack against the external network environment. Additionally, a penetration test and vulnerability assessment is conducted to identify and exploit security weaknesses. **Reputational Threat Exposures** - Using information available on the public Internet (e.g. search engines, social media, etc.), Vonahi Security attempted to discover information that could potentially harm Mobly's reputation. This includes publicly disclosed information that may or may not be useful for an attack. **External Network Penetration Test** - A penetration test was conducted to identify the potential impact of exploiting any identified vulnerabilities. Only exploits that are deemed safe were executed during this phase. Information obtained from within the Reputational Threats Exposure phase were used as part of this penetration test. **Vulnerability Assessment** - A vulnerability assessment was also performed against the list of systems provided for the scope for testing. This vulnerability assessment attempted to identify, but not exploit, security vulnerabilities that exist within the environment.

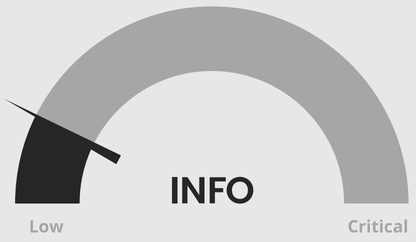
Engagement Statistics

The information below displays overall statistics that were recorded as part of this engagement. Following the statistics, Vonahi Security has summarized all of the threats identified.

External Network Security Assessment

The information below provides a high-level overview of the assessment results recorded as part of this engagement. Following this section is a summary of all the threats identified and their potential risk to your organization.

Overall Severity Ranking



ASSESSMENT SCHEDULE

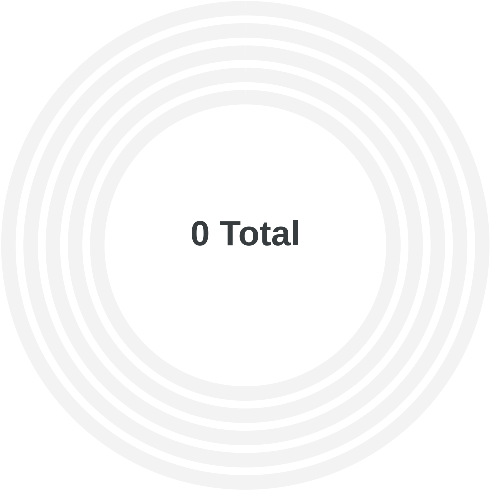
Mon, September 16, 2024
12:44 PM MT

An informational threat ranking does not pose a significant threat to the environment and are, often times, more valuable when combined with other attack vectors, such as social engineering, phishing, etc. These attacks do not directly pose a significant risk.

Engagement Results Charts

To help Mobly understand the severity of the threats identified during testing, Vonahi Security has included an over-all summary chart below that displays a comparison of the report findings as well as the vulnerabilities that were discovered.

External Network Security Assessment Results



PenTest Findings

The following chart displays the overall severity of the report findings that were documented as part of the penetration testing efforts.

C	0 CRITICAL	H	0 HIGH
M	0 MEDIUM	L	0 LOW
I	0 INFO		

As part of the penetration test, Vonahi Security also performed a vulnerability assessment to provide additional value and insight as to the vulnerabilities that were identified by our vulnerability scanner. This vulnerability scan included the discovery of common security vulnerabilities that are publicly documented with Common Vulnerabilities and Exposures (CVE) scores.

VULNERABILITY ASSESSMENT FINDINGS

5 TOTAL

0 CRITICAL	0 HIGH	1 MEDIUM	0 LOW	4 INFO

Engagement Results Summary

To summarize the results, Vonahi Security has grouped all of the findings from the penetration test into rollup findings. These rollup findings can be used to quickly determine the root cause of the issues identified in the technical report. By implementing a remediation strategy for the findings based on the rollup issues identified below, Mobly's security posture would be greatly reduced.

External Network Security Assessment

Category	Summary
N/A	N/A

Remediation Roadmap

For each assessment conducted, Vonahi Security provided a remediation roadmap to help Mobly understand the issues within the respective environment and the overall remediation strategies that should be implemented to resolve the issues identified during the penetration test. It should be noted that the remediation strategies below apply to multiple issues identified within the technical report and can greatly reduce the overall attack surface once successfully implemented.

External Network Security Assessment

Issue	Remediation Strategy
N/A	N/A

Threat Severity Rankings

To assist the organization with prioritizing findings, the findings and observations have been categorized with threat severity rankings based on the following guidelines:

SEVERITY		DESCRIPTION
▂▃▄▅▆	Critical	A critical threat ranking requires immediate remediation or mitigation. Exploiting these vulnerabilities require a minimal amount of effort by the adversary but poses a significant threat to the confidentiality, integrity, and/or availability of the organization's systems and data. A successful compromise of findings of this ranking leads to access to multiple systems and/or several pieces of sensitive information.
▂▃▄▅▆	High	A high threat ranking requires immediate remediation or mitigation. Exploiting these vulnerabilities require a minimal amount of effort by the adversary but poses a significant threat to the confidentiality, integrity, or availability of the organization's systems or data. A successful compromise of findings of this ranking leads to access to a single system or limited sensitive information.
▂▃▄▅▆	Medium	A medium threat ranking requires remediation or mitigation within a short and reasonable amount of time. These findings typically lead to a compromise of non-privileged user accounts on systems and/or applications or denote a denial-of-service (DoS) condition of the host, service, or application.
▂▃▄▅▆	Low	A low threat ranking requires remediation or mitigation once all higher prioritized findings have been remediated. These findings typically leak information to unauthorized or anonymous users and may lead to more significant attacks when combined with other attack vectors.
▂▃▄▅▆	Informational	An informational threat ranking does not pose a significant threat to the environment and may just be findings that could potentially disclose valuable information but do not expose the organization to any technical attacks. Findings rated as informational may be useful for an attacker performing information gathering on the organization to leverage in other attacks, such as social engineering or phishing.

Discovered Threats

DISCOVERED THREATS	THREAT SEVERITY RANKINGS	
External Network Security Assessment (0)		
N/A	N/A	N/A

MITRE ATT&CK Mappings

This section of the report contains details about the tactics, techniques, and procedures as defined by the MITRE ATT&CK Framework. For additional details relating to these tactics, techniques, and procedures (TTPs), Vonahi Security recommends that Mobly visit the specific URLs provided within the table below. Furthermore, Vonahi Security has also elaborated on how these TTPs were used during the penetration test in this report's Penetration Test Narrative section.

Vonahi Security recommends Mobly thoroughly leverage this report section to investigate and improve network security policies, procedures, and controls within the organization's environment. All of the attacks mentioned in this report section should have been detected and properly logged for investigation purposes by the organization.

MITRE | ATT&CK®

Time	Name	Tactic	TTPID
Mon, Sep 16, 2024 @ 12:51:52 PM MDT	Active Scanning: Scanning IP Blocks	Reconnaissance	T1595.001
Mon, Sep 16, 2024 @ 12:51:52 PM MDT	Network Service Discovery	Discovery	T1046

Reputational Threat Findings

This section addresses information that was discovered when performing information gathering about the organization. This information includes data that could be leveraged by an adversary to perform an attack, including social engineering attacks. Findings in this area focus on identifying vulnerabilities that could be used to affect the reputation, brand image, or users of the organization's various external presences.

The threat severity ranking of each finding is based on the recommended priority and order of importance as outlined in this section.

Tasks Performed

To fully assess the organization for reputational threats, Vonahi Security performed the following tasks as part of this phase of testing:

TASK PERFORMED	DOMAIN(S) ASSESSED
Performed Information Gathering: Whois, NSLookup, and ARIN Queries	www.getmobly.com
Performed DNS Enumeration for Hostnames	www.getmobly.com
Performed Username and Email Address Harvesting	www.getmobly.com
Performed Doppelganger Domain Searches	www.getmobly.com
Performed Derogatory Domain Searches	www.getmobly.com

Informational

Domain Information Gathering

Observation

One of the first things that an attacker does to gather information about an organization is perform lookups of their domain names, identify subdomains, mail servers, etc. The objective of this process is to gather as much information about the target domain so that an attacker could begin to map out the external environment of the organization. Such information could then later be used in an attack, such as social engineering.

Vonahi Security also reviewed DNS records to determine if any email spam controls are in place. This is accomplished by the use of DMARC and SPF records. Once implemented, email servers that receive emails from your domain will double check your domain's DNS records to determine if the originating email is from an authorized source. If not, the email may be completely dropped or moved to the spam folder.

Recommendation

No recommendation is necessary for this particular finding. This finding is solely information that was gathered by the consultant as part of this penetration test engagement.

Evidence

The following table displays a list of domains that were discovered using public resources:

SUB DOMAIN	IP ADDRESS
hub.getmobly.com	199.36.158.100
core-api.getmobly.com	34.144.221.185
enrichment-staging.getmobly.com	199.36.158.100
core-api.dev.getmobly.com	34.120.13.207
enrichment-tools-api.getmobly.com	34.128.178.73
hub-staging.getmobly.com	199.36.158.100
go.getmobly.com	199.60.103.225
pay.getmobly.com	34.234.126.233
enrichment.getmobly.com	199.36.158.100
admin.getmobly.com	199.36.158.100
client.getmobly.com	199.36.158.100
api.getmobly.com	216.239.36.21
admin-staging.getmobly.com	199.36.158.100
help.getmobly.com	104.18.37.238
dashboard-staging.getmobly.com	199.36.158.100
dev-api.getmobly.com	216.239.36.21
atlantis.getmobly.com	34.160.102.8

client-staging.getmobly.com	199.36.158.100

Furthermore, the consultant reviewed the DNS records provided by the domains and subdomains discovered to attempt identifying if any valuable information could be obtained. No sensitive information has been discovered from this information.

SUB DOMAIN	RECORD TYPE	DATA
www.getmobly.com	SOA	ns-1078.awsdns-06.org
www.getmobly.com	CNAME	www.getmobly.com
www.getmobly.com	CNAME	proxy-ssl.webflow.com
www.getmobly.com	A	3.233.126.24
www.getmobly.com	A	34.234.52.18
www.getmobly.com	A	52.206.163.162
www.getmobly.com	SOA	ns-cloud-a1.googledomains.com
www.getmobly.com	NS	ns-cloud-a1.googledomains.com
www.getmobly.com	NS	ns-cloud-a2.googledomains.com
www.getmobly.com	NS	ns-cloud-a3.googledomains.com
www.getmobly.com	NS	ns-cloud-a4.googledomains.com
www.getmobly.com	MX	alt1.aspmx.l.google.com
www.getmobly.com	MX	aspmx.l.google.com
www.getmobly.com	MX	alt2.aspmx.l.google.com
www.getmobly.com	MX	alt3.aspmx.l.google.com
www.getmobly.com	MX	alt4.aspmx.l.google.com
www.getmobly.com	A	75.2.70.75
www.getmobly.com	A	99.83.190.102
www.getmobly.com	TXT	google-site-verification=T7Pe3NegRe-IFD8x72nAaCxroSsZ2V4wCnUQKoTNGYU
www.getmobly.com	TXT	v=spf1 include:_spf.google.com include:123456.spf03.hubspotemail.net ~all
www.getmobly.com	TXT	v=DMARC1; p=none;

Informational

Doppelganger Domains

Observation

A Doppelganger domain is a domain that has been registered by an adversary that takes advantage of common typing mistakes or browser assumptions that target a legitimate domain. As an example, a common doppelganger domain for "www.abc.com" would be to register "wwwabc.com" or even "www.abccom.com".

Doppelganger domains have a potent impact when leveraged via email or bogus websites, as adversaries could potentially gather information such as trade secrets, usernames and passwords, and other employee information during social engineering attacks. Additionally, doppelganger domains have been commonly used to spread malware to users who accidentally misspell a legitimate domain in their web browser.

During testing against targeted domains, four (4) doppelganger domains were discovered to be registered. Mobly's network staff should review these results and determine the legitimacy of these domains.

Recommendation

By leveraging tools such as URLCrazy, your organization may perform its own periodic review of its domains to determine if anyone has attempted to register a doppelganger domain. If a doppelganger domain is discovered, gather the registrar information, and lodge a complaint with the registrar to have the doppelganger domain removed or registered to your organization.

Additionally, it is recommended that your organization register the most common variations of its domain names and spellings as a preemptive measure to combat this form of attack.

Furthermore, the organization may consider implementing a blacklist in its mail server configuration to ensure that these doppelganger domains are not used to send phishing emails to the organization.

Evidence

MISSPELLING TECHNIQUE	DOMAIN NAME	IP ADDRESS ASSOCIATED WITH DOMAIN	COUNTRY
*original	www.getmobly.com	3.233.126.24	United States
omission	www.getmoby.com	143.198.32.34	Canada
omission	www.getmobl.com	64.98.135.41	United States
replacement	www.getjobly.com	198.187.31.75	United States
subdomain	www.getmo.bly.com	67.225.139.173	United States

Sep 2024 Pen Test

Engagement Scope of Work

Through discussions with Mobly's staff, the following target applications, IP addresses, and/or ranges were included as part of the engagement scope.

IP ADDRESSES & RANGES			
99.83.190.102 (getmobly.com)			

Mobly's IT staff also provided Vonahi Security with IP addresses and ranges to exclude. The following table displays the list of excluded systems.

EXCLUDED IP ADDRESSES & RANGES			
proxy-ssl.webflow.com. (www.getmobly.com)			

Agent Information

To perform this assessment, Vonahi Security used an agent consisting of the necessary tools to conduct discovery, enumeration, attacks, etc. The agent used in this assessment contained the following information:

DESCRIPTION	DETAILS
Agent Name	External Agent
Public IP Address	54.157.67.248

Task Performed

To assess the targets listed above fully, Vonahi Security performed the following tasks:

TASK PERFORMED	DEVICES/LOCATIONS ASSESSED
Performed information gathering: NSlookup, and Ping/SNMP sweeping	All targets
Performed port scans	All active targets identified
Performed vulnerability scanning	All active targets identified
Performed web application vulnerability testing	Active/Select targets
Performed vulnerability validation	All active targets identified
Performed penetration testing	Active/Select targets

Rules of Engagement

Vonahi Security and Mobly agreed to the following rules of engagements:

ACTIVITY	DEFINITION	PERMISSION
Exploitation	Vonahi Security consultants will cautiously execute exploitation techniques to gain access to sensitive data and/or systems.	Yes
Post Exploitation	If exploitation is successful, Vonahi Security will attempt to escalate privileges within the environment to gain further access to systems	Yes

	and/or data.	

The following activities were either disabled or reduced as part of the penetration testing engagement to comply with the scope requirements:

ACTIVITY	CONFIGURED SETTING	RECOMMENDED
Password Guessing Limit Against Database Services	1	3
Password Guessing Limit Against Domain Accounts	1	2
Password Guessing Limit Against Other Network Services	1	3

Penetration Test Narrative

This phase of the external network penetration test describes some of the actions performed as part of the penetration test, including host discovery, enumeration, exploitation, and post-exploitation (if opportunities were identified). It should be noted that this portion of the report does not represent the entire list of activities that were performed as part of this assessment, primarily just those that led to some level of access, significant exposure to information, and other activities relevant to the goal of the assessment.

Host Discovery

The first process that was performed during the penetration test was host discovery. Host discovery includes several tasks, including port scanning and ping sweeps, to identify the active systems within the environment. This is a crucial step in the penetration test as it allows attackers to determine what systems are active within the targeted IP addresses and/or ranges.

Of the one (1) IP address/range that was provided as part of the scope, Vonahi Security was able to identify a total of one (1) system to be active within the targeted environment.

MITRE | ATT&CK®	
Name	Active Scanning: Scanning IP Blocks
Tactic	Reconnaissance
TTP ID	T1595.001
Note	Vonahi Security also performed a port scan against one (1) target to identify opened ports and running services. Port scanning is also important in that it allows one to identify which ports are opened and visible from the tested system. By discovering opened ports within the environment, it is then possible to determine which services are running and if any of the running services are vulnerable.

Of the one (1) address/range that was scanned, Vonahi Security found two (2) ports opened.

Enumeration

After identifying the available hosts within the network, the next phase is to conduct enumeration. Enumeration consists of scanning the identified ports to determine what services are running. Additional scans are performed based on the running services to attempt enumerating information from the running services (if possible). Such information may be useful for identifying additional vulnerabilities or knowledge for performing an attack against the service.

To help understand the operating systems and ports that were found to be most common within the environment, the following tables display the top 10 operating systems and top 10 ports.

PORT/PROTOCOL	COUNT
443/tcp	1
80/tcp	1

Targeting one (1) web application identified running on port 443/tcp, Vonahi Security performed a hidden directory brute force scan to determine if any directories could be identified that may contain sensitive information. During this process, an attacker would usually provide a wordlist containing common names, such as "administrator", "admin", "login", and more. Depending on whether or not one of the web services has a directory containing these common names, the attacker would then attempt to log in or enumerate additional information that may aid other attacks.

After completing the directory enumeration scan on port 443, Vonahi Security was unable to identify any directories that contain information that may be valuable to an attacker.

Targeting one (1) web application identified running on port 80/tcp, Vonahi Security performed a hidden directory brute force scan to determine if any directories could be identified that may contain sensitive information. During this process, an attacker would usually provide a wordlist containing common names, such as "administrator", "admin", "login", and more. Depending on whether or not one of the web services has a directory containing these common names, the attacker would then attempt to log in or enumerate additional information that may aid other attacks.

After completing the directory enumeration scan on port 80, Vonahi Security was unable to identify any directories that contain information that may be valuable to an attacker.

External Network Environment Exposures

This phase of the security assessment focused on the security of network assets within the external network environment. During this phase, Vonahi Security used a comprehensive set of tools, custom scripts, and manual techniques to thoroughly identify possible threats to the environment. Like a traditional penetration test, all identified threats were tested and validated to evaluate the depth of compromise. Unlike a traditional penetration test, this evaluation of threats was not isolated or limited to a handful of threats, but rather across all threats identified.

Informational	No Findings Identified

Observation

During testing, Vonahi Security did not identify any security vulnerabilities that could pose a threat to the organization's network environment. Although no findings were present in this testing phase, it should be noted that this assessment strictly performed testing of the environment, not including thorough web application penetration testing.

Although a more thorough list of activities performed during this network penetration test can be identified within the methodology document provided as part of the contract, some of the activities below were performed depending on the opened ports and available services exposed to the public Internet environment:

- Open-source Intelligence (OSINT) Gathering
  - Information such as employees that belong to the organization were identified using publicly available resources and social media.
  - DNS information was also enumerated in an attempt to discover additional domains and subdomains that may belong to the organization.
- Host discovery and enumeration
  - Ping sweeps as well as port scans were used to aid in the host identification process.
- Port scanning and service enumeration
  - A scan of common ports were identified including SMTP, FTP, Telnet, RDP, HTTP(s), LDAP, NFS, SMB, etc.
  - Uncommon ports were also scanned to attempt identifying services that are listening on non-standard ports.
- Vulnerability scanning (results included in the Vulnerability Report)
  - Vulnerability scans are performed as part of this network penetration test; however, the results are only included within the vulnerability tracking spreadsheet and are attached to specific report findings if any manual findings were identified as part of this assessment.
- Manual and automated penetration testing techniques, including:
  - Authentication-based attacks against network services
  - Limited authentication-based attacks against network services, specifically mail services and any authentication prompts that require Basic or NTLM authentication.
  - Man-in-the-middle attacks, including ARP poisoning
  - DNS poisoning attacks including NBNS, mDNS, and LLMNR
  - IPv6 poisoining

The lack of findings identified during this penetration test is evident that Mobly is applying effort to ensure that the network environment does not contain any threats that could be leveraged by an external attacker.

Appendix A: Host Discovery (Operating Systems)

External Network Security Assessment

During testing, it was not possible to discover the specific operating systems running on the in-scope targets. This indicates that the targets are configured correctly to not disclose sensitive operating system information, which could be extremely valuable to an attacker looking to exploit vulnerabilities in known operating systems.

Appendix B: Identified Nodes Without Ports

During testing, all identified systems were found to have at least one (1) open port. As a result, no table will be displayed in this section.

Appendix C: Host Discovery (Opened Ports)

External Network Security Assessment

IP Address	DNS Name	Port	Protocol
99.83.190.102		80	tcp
99.83.190.102		443	tcp

Discovered Vulnerabilities

The following table displays a summary of the vulnerabilities that were discovered as part of this engagement.

DISCOVERED VULNERABILITIES	THREAT SEVERITY RANKINGS
External Network Security Assessment (5)	
HSTS Missing From HTTPS Server (RFC 6797)	Medium
HSTS Missing From HTTPS Server	Informational
SSL Perfect Forward Secrecy Cipher Suites Supported	Informational
SSL/TLS Recommended Cipher Suites	Informational
TLS ALPN Supported Protocol Enumeration	Informational

Vulnerability Findings

This section of the report contains all of the vulnerabilities that were discovered for each component conducted throughout the vulnerability assessment.

External Network Vulnerability Assessment

Engagement Scope of Work

Through discussions with Mobly's staff, the following target applications, IP addresses, and/or ranges were included as part of the engagement scope.

IP ADDRESSES & RANGES			
99.83.190.102			

Mobly's IT staff also provided Vonahi Security with IP addresses and ranges to exclude. The following table displays the list of excluded systems.

EXCLUDED IP ADDRESSES & RANGES			
proxy-ssl.webflow.com.			

HSTS Missing From HTTPS Server (RFC 6797)	
Severity	▮▮▮▯▯
Description	The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections. The remote web server is not enforcing HSTS, as defined by RFC 6797.
CVSS	5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)
CVSS3	6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)
Recommendation	Configure the remote web server to use HSTS.
References	https://tools.ietf.org/html/rfc6797
Affected Nodes	99.83.190.102 on port 443/tcp

Additional Output	`HTTP/1.1 403 Forbidden`
	`Date: Mon, 16 Sep 2024 18:57:15 GMT`
	`Content-Type: text/html`
	`Content-Length: 552`
	`Connection: close`
	
	`The remote HTTPS server does not send the HTTP`
	`Strict-Transport-Security header.`

HSTS Missing From HTTPS Server	
Severity	▮▯▯▯▯
Description	The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections. The remote web server is not enforcing HSTS.
Recommendation	Configure the remote web server to use HSTS.
References	https://tools.ietf.org/html/rfc6797
Affected Nodes	99.83.190.102 on port 443/tcp

Additional Output	`HTTP/1.1 403 Forbidden`
	`Date: Mon, 16 Sep 2024 18:57:15 GMT`
	`Content-Type: text/html`
	`Content-Length: 552`
	`Connection: close`
	
	`The remote HTTPS server does not send the HTTP`
	`Strict-Transport-Security header.`

SSL Perfect Forward Secrecy Cipher Suites Supported	
Severity	▮▯▯▯▯
Description	The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the servers private key is compromised. The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.
Recommendation	n/a
References	https://www.openssl.org/docs/manmaster/man1/ciphers.html https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

	https://en.wikipedia.org/wiki/Perfect_forward_secrecy
Affected Nodes	99.83.190.102 on port 443/tcp

Additional Output

```
Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)           SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)           SHA384
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)           SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)           SHA384
    ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8       ECDH          RSA      ChaCha20-Poly1305(256) SHA256

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message
------------ snipped ------------
```

SSL/TLS Recommended Cipher Suites

Severity	▮▯▯▯▯
Description	The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites: TLSv1.3: - 0x13,0x01 TLS13_AES_128_GCM_SHA256 - 0x13,0x02 TLS13_AES_256_GCM_SHA384 - 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256 TLSv1.2: - 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256 - 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256 - 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384 - 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384 - 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305 - 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305 This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years. The remote host advertises discouraged SSL/TLS ciphers.
Recommendation	Only enable support for recommened cipher suites.
References	https://wiki.mozilla.org/Security/Server_Side_TLS https://ssl-config.mozilla.org/
Affected Nodes	99.83.190.102 on port 443/tcp

Additional Output

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined belo
w:


  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)           SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)           SHA384

The fields above are :
  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

TLS ALPN Supported Protocol Enumeration

Severity	▮▯▯▯▯
Description	The remote host supports the TLS ALPN extension. This plugin enumerates the protocols the extension supports. The remote host supports the TLS ALPN extension.
Recommendation	n/a
References	https://tools.ietf.org/html/rfc7301
Affected Nodes	99.83.190.102 on port 443/tcp

Additional Output	`http/1.1`
	`  h2`