TRIAGINGX - Vul. Pentest - 07/15/2024

Statement of Confidentiality

This document contains confidential trade secrets and proprietary information of TriagingX. The recipient is expected to treat this document as they would their own confidential internal material. Neither this document, nor any diagrams contained in this document, may be disclosed to any person outside of the recipient's organization without express written permission from TriagingX. By accepting this document, the recipient affirms that they will comply with these expectiations.

Copyright

This unpublished material contains trade secrets and other confidential information, protected under a confidentiality agreement. Unauthorized possession, use, reproduction, distribution, display, or disclosure of this material or its information is strictly prohibited.

The methodology used for auditing computer systems is considered proprietary intellectual property of TriagingX. It may not be disclosed without written permission from TriagingX. However, permission is granted to copy this report for internal dissemination within your organization or for submission to any regulatory agency.

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	ptadmin
Title	Chief Security Strategist
Office	SanJose
Email	[redacted]

Target Information

Name	Value
Target Name	MyTest123
Target IPs	["[redacted]"]
Target URLs	["[redacted]"]
Target Id	fa658223-ad26-4ec8-928e-381c9ba5161f
Case Id	9e6bf225-04ac-47fe-bb1e-2f4fcb73db19
Exploit	true
Internal	false
Investigator	ptadmin
Organization	TriagingX
Version	3.4.2.053
Start Time	2024-07-15 20:24:27

Discovered Vulnerabilities

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

DISCOVERED VULNERABILITIES	PORT/PROTOCOL	THREAT	Severity
http-title: Page Not Foundtls-nextprotoneg: http/1.1tls-al ...	443/tcp	High	●●●●●
http-server-header: nginx/1.10.3 (Ubuntu)http-title: \xE8\x ...	80/tcp	High	●●●●●
ssh-hostkey: 2048 90:25:86:55:a7:f4:37:21:19:99:38:08:81:2 ...	22/tcp	High	●●●●●
Path "/" does not require authentication	80/tcp	High	●●●●○
Path "/" does not require authentication	80/tcp	High	●●●●○
dns-nsid: bind.version: dnsmasq-2.83	53/tcp	High	●●●●○
TLSv1.0: ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_S ...	443/tcp	High	●●●●○
Spidering limited to: maxpagecount=40; withinhost=[redacted]..	443/tcp	High	●●●●○
/admin/index.html: Possible admin folder /home.html: Possib ...	80/tcp	High	●●●●○
Directory structure: Longest directory structure: Depth: ...	80/tcp	High	●●●●○
Missing 'Secure' Cookie Attribute (HTTP)	443/tcp	Medium	●●●○○
Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	2266/tcp	Medium	●●●○○
DNS Cache Snooping Vulnerability (UDP) - Active Check	53/udp	Medium	●●●○○
DNS Amplification Attacks (UDP)	53/udp	Medium	●●●○○
SSL/TLS: Certificate Expired	9443/tcp	Medium	●●●○○
SSL/TLS: Certificate In Chain Expired	443/tcp	Medium	●●●○○
Sensitive File Disclosure (HTTP)	443/tcp	Medium	●●●○○
SSL/TLS: Certificate Expired	443/tcp	Medium	●●●○○
Sensitive File Disclosure (HTTP)	443/tcp	Medium	●●●○○
Sensitive File Disclosure (HTTP)	443/tcp	Medium	●●●○○
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	443/tcp	Medium	●●●○○
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	8443/tcp	Medium	●●●○○
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	443/tcp	Medium	●●●○○
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	8443/tcp	Medium	●●●○○
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	443/tcp	Medium	●●●○○
Weak Encryption Algorithm(s) Supported (SSH)	2266/tcp	Medium	●●●○○
cpe:/a:mysql:mysql	3306/tcp	Medium	●●●○○
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	443/tcp	Medium	●●●○○

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 TRIAGINGX staff, the following target applications, IP addresses, and/or ranges were included as part of the engagement scope.

	IP ADDRESSES & RANGES
IPs	[redacted]
URLs	[redacted]

Missing 'Secure' Cookie Attribute (HTTP)

Name	Value
Severity	▁▂▃▄▅
Threat	Medium
Host	47.103.77.215
CVSSv2	AV:N/AC:L/Au:N/C:P/I:P/A:N
Output	The cookies: Set-Cookie: car_mall_session=Hvx06NJ5oo7kiuYDc2vm23GEN6nzCoTftTSuuw74; expires=Tue, 16-Jul-2024 06:40:25 GMT; Max-Age=***replaced***; path=/; httponly are missing the "Secure" cookie attribute.
Detect	Checks all cookies sent by the remote HTTP web server / application over a SSL/TLS connection for a missing 'Secure' cookie attribute.
Insight	The flaw exists if a cookie is not using the 'Secure' cookie attribute and is sent over a SSL/TLS connection. This allows a cookie to be passed to the server by the client over non-secure channels (HTTP) and subsequently allows an attacker to e.g. conduct session hijacking attacks.
References	url: https://www.rfc-editor.org/rfc/rfc6265#section-5.2.5 url: https://owasp.org/www-community/controls/SecureCookieAttribute url: https://wiki.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-002)
Recommendation	Set the 'Secure' cookie attribute for any cookies that are sent over a SSL/TLS connection.
Summary	The remote HTTP web server / application is missing to set the 'Secure' cookie attribute for one or more sent HTTP cookie.
Affected	Any web application accessible via a SSL/TLS connection (HTTPS) and at the same time also accessible over a cleartext connection (HTTP).
Port	443/tcp
Vulnerability	Missing 'Secure' Cookie Attribute (HTTP)

Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

Name	Value
Severity	▁▂▃▄▅
Threat	Medium
Host	96.74.99.149
CVSSv2	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
Output	The remote SSH server supports the following weak KEX algorithm(s): KEX algorithm | Reason --- diffie-hellman-group-exchange-sha1 | Using SHA-1

Name	Value
	diffie-hellman-group1-sha1 | Using Oakley Group 2 (a 1024-bit MODP group) and SHA-1
Detect	Checks the supported KEX algorithms of the remote SSH server. Currently weak KEX algorithms are defined as the following: - non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime - ephemerally generated key exchange groups uses SHA-1 - using RSA 1024-bit modulus key
Impact	An attacker can quickly break individual connections.
Insight	- 1024-bit MODP group / prime KEX algorithms: Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime. A nation-state can break a 1024-bit prime.
References	url: https://weakdh.org/sysadmin.html url: https://www.rfc-editor.org/rfc/rfc9142.html url: https://www.rfc-editor.org/rfc/rfc9142.html#name-summary-guidance-for-implem url: https://datatracker.ietf.org/doc/html/rfc6194
Recommendation	Disable the reported weak KEX algorithm(s) - 1024-bit MODP group / prime KEX algorithms: Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.
Summary	The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).
Port	2266/tcp
Vulnerability	Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

DNS Amplification Attacks (UDP)

Name	Value
Severity	▮▮▮▯▯
Threat	Medium
Host	47.103.77.215
CVSSv2	AV:N/AC:L/Au:N/C:N/I:N/A:P
Output	We have sent a DNS request of 17 bytes and received a response of 492 bytes.
Detect	Sends a crafted UDP based DNS request and checks the response. Note: This VT is only reporting a vulnerability if the target system / service is accessible from a public WAN (Internet) / public LAN. A configuration option 'Network type' to define if a scanned network should be seen as a public LAN can be found in the preferences of the following VT:

Name	Value
	Global variable settings (OID: 1.3.6.1.4.1.25623.1.0.12288)
Insight	A Domain Name Server (DNS) Amplification attack is a popular form of Distributed Denial of Service (DDoS) that relies on the use of publicly accessible open recursive DNS servers to overwhelm a victim system with DNS response traffic. The basic attack technique consists of an attacker sending a DNS name lookup request to an open recursive DNS server with the source address spoofed to be the victim's address. When the DNS server sends the DNS record response, it is sent instead to the victim. Attackers will typically submit a request for as much zone information as possible to maximize the amplification effect. Because the size of the response is typically considerably larger than the request, the attacker is able to amplify the volume of traffic directed at the victim. By leveraging a botnet to perform additional spoofed DNS queries, an attacker can produce an overwhelming amount of traffic with little effort. Additionally, because the responses are legitimate data coming from valid servers, it is especially difficult to block these types of attacks. Note: This finding might be an acceptable risk if you: - trust all clients which can reach the server - do not allow recursive queries from outside your trusted client network
References	cve: CVE-2006-0987 url: http://www.us-cert.gov/ncas/alerts/TA13-088A url: http://www.isotf.org/news/DNS-Amplification-Attacks.pdf
Recommendation	There are multiple possible mitigation steps depending on location and functionality needed by the DNS server: - Disable recursion - Don't allow public access to DNS Servers doing recursion - Leave recursion enabled if the DNS Server stays on a corporate network that cannot be reached by untrusted clients
Summary	A misconfigured Domain Name System (DNS) server can be exploited to participate in a Distributed Denial of Service (DDoS) attack.
Port	53/udp
Vulnerability	DNS Amplification Attacks (UDP)

Sensitive File Disclosure (HTTP)

Name	Value
Severity	▮▮▮▯▯
Threat	Medium
Host	47.103.77.215
CVSSv2	AV:N/AC:L/Au:N/C:P/I:N/A:N
Output	The following files containing sensitive information were identified: Description: Microsoft IIS / ASP.NET Core Module web.config file accessible. This could contain sensitive information about the structure of the application / web server and shouldn't be accessible. Match: <configuration> <system.webServer> Used regex: ^\s*<(configuration|system\.web(Server)?)> Extra match 1: </system.webServer> </configuration> Used regex: ^\s*</(configuration|system\.web(Server)?)> URL: https://www.[redacted]/web.config

Name	Value
Detect	Enumerate the remote web server and check if sensitive files are accessible.
Impact	Based on the information provided in these files an attacker might be able to gather additional info and/or sensitive data like usernames and passwords.
Recommendation	The sensitive files shouldn't be accessible via a web server. Restrict access to it or remove it completely.
Summary	The script attempts to identify files containing sensitive data at the remote web server like e.g.: - software (Blog, CMS) configuration or log files - web / application server configuration / password files (.htaccess, .htpasswd, web.config, web.xml, ...) - Cloud (e.g. AWS) configuration files - database backup files - SSH or SSL/TLS Private-Keys
Port	443/tcp
Vulnerability	Sensitive File Disclosure (HTTP)

Sensitive File Disclosure (HTTP)

Name	Value
Severity	▂▃▄▅▆
Threat	Medium
Host	47.103.77.215
CVSSv2	AV:N/AC:L/Au:N/C:P/I:N/A:N
Output	The following files containing sensitive information were identified: Description: Microsoft IIS / ASP.NET Core Module web.config file accessible. This could contain sensitive information about the structure of the application / web server and shouldn't be accessible. Match: <configuration> <system.webServer> Used regex: ^\s*<(configuration|system\.web(Server)?)> Extra match 1: </system.webServer> </configuration> Used regex: ^\s*</(configuration|system\.web(Server)?)> URL: https://www.[redacted]/web.config
Detect	Enumerate the remote web server and check if sensitive files are accessible.
Impact	Based on the information provided in these files an attacker might be able to gather additional info and/or sensitive data like usernames and passwords.
Recommendation	The sensitive files shouldn't be accessible via a web server. Restrict access to it or remove it completely.
Summary	The script attempts to identify files containing sensitive data at the remote web server like e.g.: - software (Blog, CMS) configuration or log files

Name	Value
	- web / application server configuration / password files (.htaccess, .htpasswd, web.config, web.xml, ...) - Cloud (e.g. AWS) configuration files - database backup files - SSH or SSL/TLS Private-Keys
Port	443/tcp
Vulnerability	Sensitive File Disclosure (HTTP)

Sensitive File Disclosure (HTTP)

Name	Value
Severity	▮▮▮▯▯
Threat	Medium
Host	47.103.77.215
CVSSv2	AV:N/AC:L/Au:N/C:P/I:N/A:N
Output	The following files containing sensitive information were identified: Description: Microsoft IIS / ASP.NET Core Module web.config file accessible. This could contain sensitive information about the structure of the application / web server and shouldn't be accessible. Match: <configuration> <system.webServer> Used regex: ^\s*<(configuration|system\.web(Server)?)> Extra match 1: </system.webServer> </configuration> Used regex: ^\s*</(configuration|system\.web(Server)?)> URL: https:/[redacted]/web.config
Detect	Enumerate the remote web server and check if sensitive files are accessible.
Impact	Based on the information provided in these files an attacker might be able to gather additional info and/or sensitive data like usernames and passwords.
Recommendation	The sensitive files shouldn't be accessible via a web server. Restrict access to it or remove it completely.
Summary	The script attempts to identify files containing sensitive data at the remote web server like e.g.: - software (Blog, CMS) configuration or log files - web / application server configuration / password files (.htaccess, .htpasswd, web.config, web.xml, ...) - Cloud (e.g. AWS) configuration files - database backup files - SSH or SSL/TLS Private-Keys
Port	443/tcp
Vulnerability	Sensitive File Disclosure (HTTP)

SSL/TLS: Certificate Expired

Name	Value
Severity	▮▮▮▯▯
Threat	Medium
Host	47.103.77.215
CVSSv2	AV:N/AC:L/Au:N/C:N/I:P/A:N
Output	The certificate of the remote service expired on 2020-09-12 23:59:59. Certificate details: fingerprint (SHA-1) | 9F36A0ED167D77EE12A23A949FABE6AE4E884BA6 fingerprint (SHA-256) | 3C558981C5AFBF57741F47444E8BE060BFED88460EF4E2D7E6E1A06B37AA0B59 issued by | CN=WoTrus DV Server CA,OU=Controlled by Sectigo exclusively for WoTrus CA Limited,O=WoTrus CA Limited,L=Shenzhen,ST=Guangdong,C=CN public key algorithm | RSA public key size (bits) | 2048 serial | 73A6444D4E2576D567F46AEDABFA21A6 signature algorithm | sha256WithRSAEncryption subject | CN=*.balingmedia.com,OU=PositiveSSL Multi-Domain,OU=Domain Control Validated subject alternative names (SAN) | *.balingmedia.com, balingmedia.com valid from | 2019-08-14 00:00:00 UTC valid until | 2020-09-12 23:59:59 UTC
Insight	This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.
Recommendation	Replace the SSL/TLS certificate by a new one.
Summary	The remote server's SSL/TLS certificate has already expired.
Port	443/tcp
Vulnerability	SSL/TLS: Certificate Expired

SSL/TLS: Certificate In Chain Expired

Name	Value
Severity	▮▮▮▯▯
Threat	Medium
Host	47.103.77.215
CVSSv2	AV:N/AC:L/Au:N/C:N/I:P/A:N
Output	The following certificates which are part of the certificate chain have expired: Subject: CN=COMODO RSA Certification Authority,O=COMODO CA Limited,L=Salford,ST=Greater Manchester,C=GB Expired on: 2020-05-30 10:48:38
Detect	Checks the expire date of the CA certificates.
Insight	Checks if the CA certificates in the SSL/TLS certificate chain have expired.
Recommendation	Sign your server certificate with a valid CA certificate.
Summary	The remote service is using a SSL/TLS certificate chain where

Name	Value
	one or multiple CA certificates have expired.
Port	443/tcp
Vulnerability	SSL/TLS: Certificate In Chain Expired

DNS Cache Snooping Vulnerability (UDP) - Active Check

Name	Value
Severity	▂▃▅▆▇
Threat	Medium
Host	47.103.77.215
CVSSv2	AV:N/AC:L/Au:N/C:P/I:N/A:N
Output	Received (an) answer(s) for a non-recursive query for "example.com". Result: 93.184.215.14
Detect	Sends a crafted DNS query and checks the response.
Impact	Attackers might gain information about cached DNS records which might lead to further attacks. Note: This finding might be an acceptable risk if you: - trust all clients which can reach the server - do not allow recursive queries from outside your trusted client network.
Insight	DNS cache snooping is when someone queries a DNS server in order to find out (snoop) if the DNS server has a specific DNS record cached, and thereby deduce if the DNS server's owner (or its users) have recently visited a specific site. This may reveal information about the DNS server's owner, such as what vendor, bank, service provider, etc. they use. Especially if this is confirmed (snooped) multiple times over a period. This method could even be used to gather statistical information - for example at what time does the DNS server's owner typically access his net bank etc. The cached DNS record's remaining TTL value can provide very accurate data for this. DNS cache snooping is possible even if the DNS server is not configured to resolve recursively for 3rd parties, as long as it provides records from the cache also to 3rd parties (a.k.a. 'lame requests').
References	url: https://www.cs.unc.edu/~fabian/course_papers/cache_snooping.pdf url: https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/dns-server-cache-snooping-attacks url: https://kb.isc.org/docs/aa-00509 url: https://kb.isc.org/docs/aa-00482
Recommendation	There are multiple possible mitigation steps depending on location and functionality needed by the DNS server: - Disable recursion - Don't allow public access to DNS Servers doing recursion - Leave recursion enabled if the DNS Server stays on a corporate network that cannot be reached by untrusted clients
Summary	The DNS server is prone to a cache snooping vulnerability.

Name	Value
Port	53/udp
Vulnerability	DNS Cache Snooping Vulnerability (UDP) - Active Check

SSL/TLS: Certificate Expired

Name	Value
Severity	▂▃▅▆▇
Threat	Medium
Host	96.74.99.146
CVSSv2	AV:N/AC:L/Au:N/C:N/I:P/A:N
Output	The certificate of the remote service expired on 2022-05-20 19:14:28. Certificate details: fingerprint (SHA-1) | BF9706752AFE5B816B2C1B3A11ECAB2B94E91D86 fingerprint (SHA-256) | 47A875EBF09377F93FDF959115978FD666AFF15C303FDD6E4A62D059AF719F3A issued by | CN=Go Daddy Secure Certificate Authority - G2,OU=http://certs.godaddy.com/repository/,O=GoDaddy.com\, Inc.,L=Scottsdale,ST=Arizona,C=US public key algorithm | RSA public key size (bits) | 2048 serial | 00C6B85331B1AD295D signature algorithm | sha256WithRSAEncryption subject | CN=*.triagingx.com,OU=Domain Control Validated subject alternative names (SAN) | *.triagingx.com, triagingx.com valid from | 2020-03-21 13:34:53 UTC valid until | 2022-05-20 19:14:28 UTC
Insight	This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.
Recommendation	Replace the SSL/TLS certificate by a new one.
Summary	The remote server's SSL/TLS certificate has already expired.
Port	9443/tcp
Vulnerability	SSL/TLS: Certificate Expired

SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Name	Value
Severity	▂▃▅▆▇
Threat	Medium
Host	96.74.99.146
CVSSv2	AV:N/AC:M/Au:N/C:P/I:N/A:N
Output	In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.
Detect	Check the used TLS protocols of the services provided by this system.

Name	Value
Impact	An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.
Insight	The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like: - CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST) - CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)
References	cve: CVE-2011-3389 cve: CVE-2015-0204 url: https://ssl-config.mozilla.org/ url: https://bettercrypto.org/ url: https://datatracker.ietf.org/doc/rfc8996/ url: https://vnhacker.blogspot.com/2011/09/beast.html
Recommendation	It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.
Summary	It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
Affected	All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.
Port	443/tcp
Vulnerability	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Name	Value
Severity	▂▃▅▆▇
Threat	Medium
Host	[redacted]
CVSSv2	AV:N/AC:M/Au:N/C:P/I:N/A:N
Output	In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.
Detect	Check the used TLS protocols of the services provided by this system.
Impact	An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.
Insight	The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:

Name	Value
	- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST) - CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)
References	cve: CVE-2011-3389 cve: CVE-2015-0204 url: https://ssl-config.mozilla.org/ url: https://bettercrypto.org/ url: https://datatracker.ietf.org/doc/rfc8996/ url: https://vnhacker.blogspot.com/2011/09/beast.html
Recommendation	It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.
Summary	It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
Affected	All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.
Port	8443/tcp
Vulnerability	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Name	Value
Severity	▂▃▅▆▇
Threat	Medium
Host	[redacted]
CVSSv2	AV:N/AC:M/Au:N/C:P/I:N/A:N
Output	In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.
Detect	Check the used TLS protocols of the services provided by this system.
Impact	An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.
Insight	The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like: - CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST) - CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)
References	cve: CVE-2011-3389 cve: CVE-2015-0204 url: https://ssl-config.mozilla.org/ url: https://bettercrypto.org/ url: https://datatracker.ietf.org/doc/rfc8996/

Name	Value
	url: https://vnhacker.blogspot.com/2011/09/beast.html
Recommendation	It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.
Summary	It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
Affected	All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.
Port	443/tcp
Vulnerability	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Name	Value
Severity	▂▃▅▆▇
Threat	Medium
Host	[redacted]
CVSSv2	AV:N/AC:M/Au:N/C:P/I:N/A:N
Output	In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.
Detect	Check the used TLS protocols of the services provided by this system.
Impact	An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.
Insight	The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like: - CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST) - CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)
References	cve: CVE-2011-3389 cve: CVE-2015-0204 url: https://ssl-config.mozilla.org/ url: https://bettercrypto.org/ url: https://datatracker.ietf.org/doc/rfc8996/ url: https://vnhacker.blogspot.com/2011/09/beast.html
Recommendation	It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.
Summary	It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
Affected	All services providing an encrypted communication using the

Name	Value
	TLSv1.0 and/or TLSv1.1 protocols.
Port	8443/tcp
Vulnerability	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Weak Encryption Algorithm(s) Supported (SSH)

Name	Value
Severity	▮▮▮▯▯
Threat	Medium
Host	96.74.99.149
CVSSv2	AV:N/AC:M/Au:N/C:P/I:N/A:N
Output	The remote SSH server supports the following weak client-to-server encryption algorithm(s): 3des-cbc aes128-cbc aes192-cbc aes256-cbc blowfish-cbc cast128-cbc The remote SSH server supports the following weak server-to-client encryption algorithm(s): 3des-cbc aes128-cbc aes192-cbc aes256-cbc blowfish-cbc cast128-cbc
Detect	Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server. Currently weak encryption algorithms are defined as the following: - Arcfour (RC4) cipher based algorithms - none algorithm - CBC mode cipher based algorithms
Insight	- The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore. - The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it. - A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.
References	url: https://www.rfc-editor.org/rfc/rfc4253#section-6.3 url: https://www.kb.cert.org/vuls/id/958563
Recommendation	Disable the reported weak encryption algorithm(s).
Summary	The remote SSH server is configured to allow / support weak encryption algorithm(s).

Name	Value
Port	2266/tcp
Vulnerability	Weak Encryption Algorithm(s) Supported (SSH)

SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Name	Value
Severity	▮▮▮▯▯
Threat	Medium
Host	47.103.77.215
CVSSv2	AV:N/AC:M/Au:N/C:P/I:N/A:N
Output	In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.
Detect	Check the used TLS protocols of the services provided by this system.
Impact	An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.
Insight	The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like: - CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST) - CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)
References	cve: CVE-2011-3389 cve: CVE-2015-0204 url: https://ssl-config.mozilla.org/ url: https://bettercrypto.org/ url: https://datatracker.ietf.org/doc/rfc8996/ url: https://vnhacker.blogspot.com/2011/09/beast.html
Recommendation	It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.
Summary	It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
Affected	All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.
Port	443/tcp
Vulnerability	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Name	Value

Name	Value
Severity	▂▃▅▆▇
Threat	Medium
Host	47.103.77.215
CVSSv2	AV:N/AC:H/Au:N/C:P/I:P/A:N
Output	Server Temporary Key Size: 1024 bits
Detect	Checks the DHE temporary public key size.
Impact	An attacker might be able to decrypt the SSL/TLS communication offline.
Insight	The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.
References	url: https://weakdh.org/ url: https://weakdh.org/sysadmin.html
Recommendation	Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references). For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.
Summary	The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).
Port	443/tcp
Vulnerability	SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Discovered Port List

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

ssh-hostkey: 2048 90:25:86:55:a7:f4:37:21:19:99:38:08:81:2 ...

Name	Value
Severity	▂▃▅▆█
Threat	High
Host	47.103.77.215
CPE	cpe:/a:openbsd:openssh:7.2p2 cpe:/o:linux:linux_kernel
Output	ssh-hostkey: 2048 90:25:86:55:a7:f4:37:21:19:99:38:08:81:23:7d:1b (RSA) 256 78:42:57:85:6b:f0:da:13:4d:bd:d9:2c:e2:e8:a9:a5 (ECDSA) 256 07:9c:d0:0e:b7:56:10:9c:7c:63:8d:04:47:73:c7:09 (ED25519)
Port	22/tcp
Service	ssh
Product	OpenSSH (7.2p2 Ubuntu 4ubuntu2.10) (Ubuntu Linux; protocol 2.0)
State	open

http-server-header: nginx/1.10.3 (Ubuntu)http-title: \xE8\x ...

Name	Value
Severity	▂▃▅▆█
Threat	High
Host	47.103.77.215
CPE	cpe:/a:igor_sysoev:nginx:1.10.3 cpe:/o:linux:linux_kernel
Output	http-server-header: nginx/1.10.3 (Ubuntu)http-title: \xE8\x8B\x8F\xE5\xB7\x9E\xE6\xB9\xBE\xE6\xA2\xA6\xE5\xB9\xBB\xE6\xB0\xB4\xE4\xB8\x96\xE7\x95\x8C\xE6\xAC\xA2\xE8\xBF\x8E\xE6\x82\xA8\xEF\xBC\x81
Port	80/tcp
Service	http
Product	nginx (1.10.3) (Ubuntu)
State	open

http-title: Page Not Foundtls-nextprotoneg: http/1.1tls-al ...

Name	Value
Severity	▂▃▅▆█

Name	Value
Threat	High
Host	47.103.77.215
CPE	cpe:/a:igor_sysoev:nginx:1.10.3 cpe:/o:linux:linux_kernel
Output	http-title: Page Not Foundtls-nextprotoneg: http/1.1tls-alpn: http/1.1ssl-date: TLS randomness does not represent timessl-cert: Subject: commonName=*.balingmedia.comSubject Alternative Name: DNS:*.balingmedia.com, DNS:balingmedia.comNot valid before: 2019-08-14T00:00:00Not valid after: 2020-09-12T23:59:59http-server-header: nginx/1.10.3 (Ubuntu)http-robots.txt: 1 disallowed entry /
Port	443/tcp
Service	http
Product	nginx (1.10.3) (Ubuntu)
State	open

dns-nsid: bind.version: dnsmasq-2.83

Name	Value
Severity	▮▮▮▮▯
Threat	High
Host	47.103.77.215
CPE	cpe:/a:thekelleys:dnsmasq:2.83
Output	dns-nsid: bind.version: dnsmasq-2.83
Port	53/tcp
Service	domain
Product	dnsmasq (2.83)
State	open

cpe:/a:mysql:mysql

Name	Value
Severity	▮▮▮▯▯
Threat	Medium
Host	47.103.77.215
CPE	cpe:/a:mysql:mysql
Port	3306/tcp
Service	mysql
Product	MySQL (unauthorized)
State	open

Discovered Exploitations

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

http-brute

Name	Value
Severity	📶
Threat	High
Host	47.103.77.215
CPE	cpe:/a:igor_sysoev:nginx:1.10.3 cpe:/o:linux:linux_kernel
Output	Path "/" does not require authentication
Port	80/tcp
Service	http
Detect	http-brute
Product	nginx (1.10.3) (Ubuntu)

http-brute

Name	Value
Severity	📶
Threat	High
Host	47.103.77.215
CPE	cpe:/a:igor_sysoev:nginx:1.10.3 cpe:/o:linux:linux_kernel
Output	Path "/" does not require authentication
Port	80/tcp
Service	http
Detect	http-brute
Product	nginx (1.10.3) (Ubuntu)

http-sitemap-generator

Name	Value
Severity	📶
Threat	High

Name	Value
Host	47.103.77.215
CPE	cpe:/a:igor_sysoev:nginx:1.10.3 cpe:/o:linux:linux_kernel
Output	Directory structure: Longest directory structure: Depth: 0 Dir: / Total files found (by extension):
Port	80/tcp
Service	http
Detect	http-sitemap-generator
Product	nginx (1.10.3) (Ubuntu)

http-enum

Name	Value
Severity	▂▃▄▅▆
Threat	High
Host	47.103.77.215
CPE	cpe:/a:igor_sysoev:nginx:1.10.3 cpe:/o:linux:linux_kernel
Output	/admin/index.html: Possible admin folder /home.html: Possible admin folder /admin.html: Possible admin folder /robots.txt: Robots file /.htaccess: Incorrect permissions on .htaccess or .htpasswd files
Port	80/tcp
Service	http
Detect	http-enum
Product	nginx (1.10.3) (Ubuntu)

http-errors

Name	Value
Severity	▂▃▄▅▆
Threat	High
Host	47.103.77.215
CPE	cpe:/a:igor_sysoev:nginx:1.10.3 cpe:/o:linux:linux_kernel
Output	[redacted] Found the following error pages: Error Code: 404 [redacted]:443/
Port	443/tcp
Service	http
Detect	http-errors
Product	nginx (1.10.3) (Ubuntu)

ssl-enum-ciphers

Name	Value
Severity	▂▃▅▆▇
Threat	High
Host	47.103.77.215
CPE	cpe:/a:igor_sysoev:nginx:1.10.3 cpe:/o:linux:linux_kernel
Output	TLSv1.0: ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - A TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (dh 1024) - A TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 2048) - A TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - A TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (dh 1024) - A TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 2048) - A compressors: NULL cipher preference: server warnings: Key exchange (dh 1024) of lower strength than certificate key TLSv1.1: ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - A TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (dh 1024) - A TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 2048) - A TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - A TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (dh 1024) - A TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 2048) - A compressors: NULL cipher preference: server warnings: Key exchange (dh 1024) of lower strength than certificate key TLSv1.2: ciphers: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 1024) - A TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (dh 1024) - A TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - A TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (dh 1024) - A TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 2048) - A TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 1024) - A TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 1024) - A TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - A TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (dh 1024) - A TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 2048) - A compressors: NULL cipher preference: server warnings: Key exchange (dh 1024) of lower strength than certificate key least strength: A
Port	443/tcp
Service	http
Detect	ssl-enum-ciphers
Product	nginx (1.10.3) (Ubuntu)