



Cyber Risk Score Report

THIS REPORT WAS GENERATED FROM THE FORTIFYDATA CYBER RISK SCORING PLATFORM. THE REPORT PROVIDES A PRECISE POINT-IN-TIME SNAPSHOT OF FORTIFYDATA'S CYBERSECURITY POSTURE AND MONITORING TRENDS OF EXTERNAL FACING ASSETS. THE SCORE WAS DEVELOPED THROUGH PERFORMING AN IN-DEPTH ASSESSMENT OF EXTERNAL FACING ASSETS AND STATISTICAL ANALYSIS OF DEMO COMPANY'S NETWORK AND APPLICATION LAYER, DARK WEB DISCOVERIES, IP REPUTATION, AND BREACH HISTORY.

Executive Summary

OVERVIEW

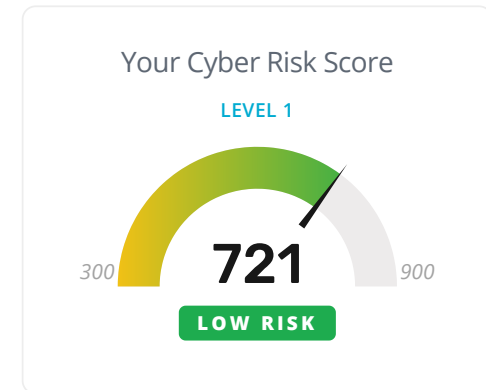
The purpose of the FortifyData Cyber Risk Score is to provide a platform capable of assessing cyber risk exposures while generating a cyber risk score for every business with an online presence. This easy to understand risk score will help Demo Company discover its cyber risk exposure through analysis of its infrastructure, applications, data breach history and compromised data sets. FortifyData's score is generated using a combination of an empirical and data-driven models, which stands out through its use of AI as part of the scoring algorithm. This includes expert opinion, from our product advisory board, that informed our machine learning model of the appropriate weighting of threat data categories to create the most accurate indicator of risk exposure.

Cyber Risk Score : **721 (Risk Level 4)**

LOW risk indicates the unlikely presence of significant cyber risks present within the company's external facing resources.

Identified low risk vulnerabilities may not pose immediate threats, but may eventually lead to significant breaches if not addressed within a reasonable time frame. Continuous monitoring of threat landscape is important to identify changes that may impact the score.

If you believe our analysis has presented one or more false positives within the findings, please contact us for validation at support@fortifydata.com.



SCOPE OF ANALYSIS

FortifyData's assessment includes cyber intelligence data analysis of the following risk areas:

External Network
Patching Cadence
Data Breach
Security Controls
Malware



Application
Dark Web
Third Party
Internal Network



CYBER RISK DISCOVERY



INFRASTRUCTURE ASSESSMENT

25 Issues

Last checked: May 04, 2021



APPLICATION ASSESSMENT

2 Issues

Last checked: May 04, 2021



BREACH HISTORY

0 Records

Last checked: May 04, 2021



DARK WEB DISCOVERY

61 Records

Last checked: May 04, 2021



CONTROL FRAMEWORK

0% Compliant

Last checked: May 04, 2021



THREAT INTELLIGENCE

0 Threats

Last checked: May 04, 2021

Resources In-Scope of Assessment

Classification	Asset Name	IP Number	Data Types In-scope
CRITICAL	ctf19.root-me.org	163.172.195.211	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
CRITICAL	ctf20.root-me.org	163.172.195.228	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
CRITICAL	ctf21.root-me.org	163.172.228.138	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
CRITICAL	ctf23.root-me.org	163.172.228.151	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
CRITICAL	ctf24.root-me.org	163.172.228.173	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
CRITICAL	ctf25.root-me.org	163.172.228.174	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
CRITICAL	ctf26.root-me.org	163.172.228.192	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
CRITICAL	ctf27.root-me.org	163.172.228.194	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
CRITICAL	ctf29.root-me.org	163.172.229.5	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
CRITICAL	ctf30.root-me.org	163.172.229.107	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
CRITICAL	ctf31.root-me.org	163.172.229.109	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL

Classification	Asset Name	IP Number	Data Types In-scope
CRITICAL	ctf32.root-me.org	163.172.229.111	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE OD L
CRITICAL	ctf34.root-me.org	163.172.229.135	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE OD L
CRITICAL	ctf36.root-me.org	163.172.230.17	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE OD L
CRITICAL	ctf38.root-me.org	163.172.230.33	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE OD L
CRITICAL	hypervisor.root-me.org	195.154.26.119	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE OD L
CRITICAL	ipv4.www.root-me.org	212.129.28.16	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE OD L
CRITICAL	irc.root-me.org	51.210.70.121	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE OD L
LOW	librenms.service.root-me.org	212.129.28.12	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE OD L
MODERATE	mail.pro.root-me.org	85.31.206.82	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
CRITICAL	pro.root-me.org	212.129.28.16	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE OD L
CRITICAL	repository.root-me.org	212.129.28.16	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE OD L

Classification	Asset Name	IP Number	Data Types In-scope
LOW	zucarita47.example.com	-	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
LOW	zfbphvtolekfnjl.example.com	-	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
LOW	zyu086201.example.com	-	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
LOW	zhourue.example.com	-	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
LOW	zimbra.home.example.com	-	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
CRITICAL	tradvio.net	-	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
CRITICAL	curry.example.com	-	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
CRITICAL	nxdomain.example.com	-	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
CRITICAL	unsubscribe.example.com	-	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
CRITICAL	www.piedpiper.com	104.18.22.192	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
CRITICAL	assets.piedpiper.com	99.84.216.201	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL

Classification	Asset Name	IP Number	Data Types In-scope
CRITICAL	piedpiper.com	104.18.23.192	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
CRITICAL	dev.piedpiper.com	104.18.23.192	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
CRITICAL	stg.piedpiper.com	44.240.150.65	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
MODERATE	www.root-me.org	212.129.28.16	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
CRITICAL	api.www.root-me.org	212.129.28.16	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
MODERATE	challenge01.root-me.org	212.129.38.224	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
MODERATE	ctf01.root-me.org	212.129.28.18	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
MODERATE	ctf02.root-me.org	212.129.28.21	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
CRITICAL	ctf03.root-me.org	212.129.29.185	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
MODERATE	ctf04.root-me.org	212.129.29.186	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
MODERATE	ctf05.root-me.org	212.129.29.187	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL

Classification	Asset Name	IP Number	Data Types In-scope
LOW	ctf06.root-me.org	212.83.142.83	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
LOW	ctf07.root-me.org	212.83.142.84	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
MODERATE	ctf08.root-me.org	212.129.39.172	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
MODERATE	ctf09.root-me.org	163.172.228.114	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
MODERATE	ctf10.root-me.org	163.172.228.224	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
MODERATE	ctf11.root-me.org	212.83.175.116	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
MODERATE	ctf14.root-me.org	212.83.175.138	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
MODERATE	ctf15.root-me.org	212.83.175.152	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
CRITICAL	ctf16.root-me.org	163.172.195.64	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
CRITICAL	ctf17.root-me.org	163.172.195.80	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
CRITICAL	ctf18.root-me.org	163.172.195.97	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL

Classification	Asset Name	IP Number	Data Types In-scope
LOW	238004.example.com	-	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
LOW	227427.example.com	-	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
LOW	204718.example.com	-	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
LOW	8027.example.com	-	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
LOW	226554.example.com	-	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
LOW	1.example.com	-	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
LOW	3.example.com	-	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
LOW	a.example.com	-	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
LOW	5.example.com	-	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
LOW	a-b.example.com	-	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL
LOW	2.example.com	-	CHD PII NPI PHI ODC IPR TRS CEM ICD ODM MKM PRE ODL

External Network Summary



Critical

1



High

2



Medium

17



Low

5

irc.root-me.org - 51.210.70.121

CRITICAL

Unix Operating System Unsupported Version Detection

Descriptions

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Solutions

Upgrade to a version of the Unix operating system that is currently supported.

Likelihood Changed

Justification

Triggering something here.

Date Adjusted

2021-04-14

irc.root-me.org - 51.210.70.121

HIGH SSL Version 2 and 3 Protocol Detection

Descriptions

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including: - An insecure padding scheme with CBC ciphers. - Insecure session renegotiation and resumption schemes. An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients. Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely. NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Solutions

Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead.

assets.piedpiper.com - 99.84.216.201

HIGH SSL Certificate Cannot Be Trusted

Descriptions

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below : - First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority. - Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates. - Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize. If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Solutions

Purchase or generate a proper SSL certificate for this service.

irc.root-me.org - 51.210.70.121

MEDIUM TLS Version 1.0 Protocol Detection

Descriptions

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible. As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solutions

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

irc.root-me.org - 51.210.70.121

MEDIUM SSL Certificate Cannot Be Trusted

Descriptions

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below : - First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority. - Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates. - Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize. If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Solutions

Purchase or generate a proper SSL certificate for this service.

www.piedpiper.com - 104.18.22.192

MEDIUM TLS Version 1.0 Protocol Detection

Descriptions

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible. As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solutions

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

assets.piedpiper.com - 99.84.216.201

MEDIUM TLS Version 1.0 Protocol Detection

Descriptions

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible. As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solutions

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

piedpiper.com - 104.18.23.192

MEDIUM TLS Version 1.0 Protocol Detection

Descriptions

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible. As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solutions

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

dev.piedpiper.com - 104.18.23.192

MEDIUM TLS Version 1.0 Protocol Detection

Descriptions

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible. As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solutions

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

irc.root-me.org - 51.210.70.121

MEDIUM SSL Medium Strength Cipher Suites Supported (SWEET32)

Descriptions

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite. Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Solutions

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

www.piedpiper.com - 104.18.22.192

MEDIUM SSL Medium Strength Cipher Suites Supported (SWEET32)

Descriptions

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite. Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Solutions

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

assets.piedpiper.com - 99.84.216.201

MEDIUM SSL Medium Strength Cipher Suites Supported (SWEET32)

Descriptions

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite. Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Solutions

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

piedpiper.com - 104.18.23.192

MEDIUM SSL Medium Strength Cipher Suites Supported (SWEET32)

Descriptions

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite. Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Solutions

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

dev.piedpiper.com - 104.18.23.192

MEDIUM SSL Medium Strength Cipher Suites Supported (SWEET32)

Descriptions

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite. Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Solutions

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

irc.root-me.org - 51.210.70.121

MEDIUM SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Descriptions

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode. MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections. As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service. The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism. This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

Solutions

Disable SSLv3. Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

irc.root-me.org - 51.210.70.121

MEDIUM SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Descriptions

The remote host supports the use of RC4 in one or more cipher suites. The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness. If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

Solutions

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

irc.root-me.org - 51.210.70.121

MEDIUM SSH Weak Algorithms Supported

Descriptions

Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

Solutions

Contact the vendor or consult product documentation to remove the weak ciphers.

mail.pro.root-me.org - 85.31.206.82

MEDIUM SSL Self-Signed Certificate

Descriptions

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host. Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solutions

Purchase or generate a proper SSL certificate for this service.

mail.pro.root-me.org - 85.31.206.82

MEDIUM TLS Version 1.0 Protocol Detection

Descriptions

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible. As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solutions

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

mail.pro.root-me.org - 85.31.206.82

MEDIUM SSL Certificate Cannot Be Trusted

Descriptions

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below : - First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority. - Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates. - Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize. If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Solutions

Purchase or generate a proper SSL certificate for this service.

irc.root-me.org - 51.210.70.121

LOW SSH Weak MAC Algorithms Enabled

Descriptions

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak. Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

Solutions

Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

irc.root-me.org - 51.210.70.121

LOW SSH Server CBC Mode Ciphers Enabled

Descriptions

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext. Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solutions

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

mail.pro.root-me.org - 85.31.206.82

LOW SSL Anonymous Cipher Suites Supported

Descriptions

The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

Solutions

Reconfigure the affected application if possible to avoid use of weak ciphers.

example.com - 93.184.216.34

LOW TLS Version 1.0 Protocol Detection

Descriptions

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible. As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solutions

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

www.example.com - 93.184.216.34

LOW TLS Version 1.0 Protocol Detection

Descriptions

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible. As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solutions

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Web Application Vulnerabilities



Critical

0



High

0



Medium

2



Low

0

www.piedpiper.com - 104.18.22.192

MEDIUM

WordPress User Enumeration

Descriptions

The version of WordPress hosted on the remote web server is affected by a user enumeration vulnerability. An unauthenticated, remote attacker can exploit this to learn the names of valid WordPress users. This information could be used to mount further attacks.

Solutions

www.piedpiper.com - 104.18.22.192

MEDIUM Web Application Potentially Vulnerable to Clickjacking

Descriptions

The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions. X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors. Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource. Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

Solutions

Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response. This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

Internal Network Summary



Critical

0



High

0



Medium

0



Low

0

Open Port Summary

Insecure Ports

SSH
22
assets tcp

SMTP
25
assets tcp

80
assets tcp

OPEN PORTS

CRITICAL Port 25 tcp/smtp

Problem
Port 25 is unsecured, and Botnet spammers can use it to send spam.

Assets
| mail.pro.root-me.org

MODERATE Port 22 tcp/ssh

Problem
Port 22 is a secure port, but should not be exposed to the world.

Assets
| irc.root-me.org | service.root-me.org

INFO Port 80 tcp/

Assets

www.root-me.org
ipv4.www.root-me.org
assets.piedpiper.com
www.piedpiper.com

api.www.root-me.org
example.com
dev.piedpiper.com
test88.root-me.org

challenge01.root-me.org
www.example.com
service.root-me.org
piedpiper.com

INFO Port 111 tcp/rpc-portmapper

Assets

irc.root-me.org

INFO Port 427 tcp/

Assets

hypervisor.root-me.org

INFO Port 443 tcp/

Assets

www.root-me.org
example.com
dev.piedpiper.com
test88.root-me.org

api.www.root-me.org
www.example.com
service.root-me.org
piedpiper.com

ipv4.www.root-me.org
assets.piedpiper.com
www.piedpiper.com

INFO Port 465 tcp/smtp

Assets

| mail.pro.root-me.org

INFO Port 902 tcp/vmware_auth

Assets

| hypervisor.root-me.org

INFO Port 993 tcp/imap

Assets

| mail.pro.root-me.org

INFO Port 2052 tcp/www

Assets

| dev.piedpiper.com

| www.piedpiper.com

| piedpiper.com

INFO Port 2053 tcp/www

Assets

| dev.piedpiper.com

| www.piedpiper.com

| piedpiper.com

Dark Web Monitoring Summary



Password
25(83%)



61

TOTAL COMPANY RECORDS EXPOSED



30

TOTAL UNIQUE EMAILS EXPOSED



25

TOTAL PASSWORDS EXPOSED



03.16.2021

LAST EXPOSED


Exposed records


Source	Type	Email	Date	Action Taken
breach_Comp_torrent_cleaned__easy_access_.41GB	stolenid breach	chad@hackthissite.org	03.16.2021	No action taken
breach_Comp_torrent_cleaned__easy_access_.41GB	stolenid breach	hackyykcah@hackthissite.org	03.16.2021	No action taken
breach_Comp_torrent_cleaned__easy_access_.41GB	stolenid breach	james@hackthissite.org	03.16.2021	No action taken
breach_Comp_torrent_cleaned__easy_access_.41GB	stolenid breach	pothead420anarchy@hackthissite.org	03.16.2021	No action taken


Source	Type	Email	Date	Action Taken
breach_Comp_torrent_cleaned__easy_access_41GB	stolenid breach	scram@hackthissite.org	03.16.2021	No action taken
Combo List 3.2B	stolenid breach	chad@hackthissite.org	02.08.2021	No action taken
Combo List 3.2B	stolenid breach	hackyykcah@hackthissite.org	02.08.2021	No action taken
Combo List 3.2B	stolenid breach	james@hackthissite.org	02.08.2021	No action taken
Combo List 3.2B	stolenid breach	pothead420anarchy@hackthissite.org	02.08.2021	No action taken
AdultFriendFinder.com	stolenid breach	manonmission@hackthissite.org	01.09.2020	No action taken
zynga.com (games Words with Friends and Draw Something)	stolenid breach	scram@hackthissite.org	12.16.2019	No action taken
Combo Pack CCRT-E-P 2.21M	stolenid breach	scram@hackthissite.org	09.18.2019	No action taken
cafepress.com	stolenid breach	umn@hackthissite.org	08.09.2019	No action taken
alora.io	stolenid breach	sam@hackthissite.org	06.18.2019	No action taken
armorgames.com	stolenid breach	scram@hackthissite.org	04.06.2019	No action taken

Source	Type	Email	Date	Action Taken
verifications.io	stolenid breach	advertising@hackthissite.org	03.01.2019	No action taken
verifications.io	stolenid breach	esnowden@hackthissite.org	03.01.2019	No action taken
verifications.io	stolenid breach	fmckinney@hackthissite.org	03.01.2019	No action taken
verifications.io	stolenid breach	jgaskin@hackthissite.org	03.01.2019	No action taken
verifications.io	stolenid breach	jhammond@hackthissite.org	03.01.2019	No action taken
verifications.io	stolenid breach	kbeaver@hackthissite.org	03.01.2019	No action taken
verifications.io	stolenid breach	kmarx@hackthissite.org	03.01.2019	No action taken
verifications.io	stolenid breach	kmitnick@hackthissite.org	03.01.2019	No action taken
verifications.io	stolenid breach	manonmission@hackthissite.org	03.01.2019	No action taken
verifications.io	stolenid breach	smcclure@hackthissite.org	03.01.2019	No action taken
verifications.io	stolenid breach	sspade@hackthissite.org	03.01.2019	No action taken

Patching Cadence Summary

 5
Critical/High Severity > 30 Days

 3
Moderate Severity > 60 Days

 1
Low Severity > 90 Days

NUMBER OF MISSING PATCHES: 9

beginnertriathlete.com>

CRITICAL

PHP 5.6.x < 5.6.39 Multiple vulnerabilities

Upgrade to PHP version 5.6.39 or later.

Vulnerability Published Date: 11/14/2018 **Patch Published Date:** 12/06/2018

store.beginnertriathlete.com>

HIGH

PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.

Upgrade to PHP version 7.3.11 or later.

Vulnerability Published Date: 10/24/2019 **Patch Published Date:** 10/24/2019

ox.beginnertriathlete.com>

HIGH

PHP 5.6.x < 5.6.40 Multiple vulnerabilities.

Upgrade to PHP version 5.6.40 or later.

Vulnerability Published Date: 01/10/2019 **Patch Published Date:** 01/10/2019

ox.beginnertriathlete.com>

HIGH

PHP 5.6.x < 5.6.34 Stack Buffer Overflow

Upgrade to PHP version 5.6.34 or later.

Vulnerability Published Date: 03/01/2018 **Patch Published Date:** 03/01/2018

ox.beginnertriathleteds.com>

HIGH

PHP 5.6.x < 5.6.36 Multiple Vulnerabilities

Upgrade to PHP version 5.6.36 or later.

Vulnerability Published Date: 04/26/2018 **Patch Published Date:** 04/26/2018

ox.beginnertriathlete.com>

MODERATE

PHP < 7.3.24 Multiple Vulnerabilities

Upgrade to PHP version 7.3.24 or later.

Vulnerability Published Date: 10/29/2020 **Patch Published Date:** 10/29/2020

ox.beginnertriathletedts.com>

MODERATE

PHP 5.6.x < 5.6.38 Transfer-Encoding Parameter XSS Vulnerability

Upgrade to PHP version 5.6.38 or later.

Vulnerability Published Date: 09/13/2018 **Patch Published Date:** 09/13/2018

ox.beginnertriathletedts.com>

MODERATE

PHP 5.6.x < 5.6.37 exif_thumbnail_extract() DoS

Upgrade to PHP version 5.6.37 or later.

Vulnerability Published Date: 06/07/2018 **Patch Published Date:** 07/19/2018

ox.beginnertriathlete.com>

LOW

PHP 5.6.x < 5.6.35 Security Bypass Vulnerability

Upgrade to PHP version 5.6.35 or later.

Vulnerability Published Date: 03/29/2018 **Patch Published Date:** 03/29/2018