Qualys. Cloud Platform

Scan Results

August 01, 2022

Report Summary	
User Name:	Lucas
Login Name:	xxxxxxx
Company:	xxxxxxx
User Role:	xxxxxxx
Address:	xxxxxx
City:	xxxxxx
Zip:	xxxxxxxx
Country:	Brazil
Created:	08/01/2022 at 03:59:20 PM (GMT-0300)
Launch Date:	08/01/2022 at 03:21:54 PM (GMT-0300)
Active Hosts:	2
Total Hosts:	2
Type:	On demand
Status:	Finished
Reference:	scan/1659378114.15293
Scanner Appliances:	teste (Scanner 12.11.22-1, Vulnerability Signatures 2.5.544-2)
Duration:	00:34:38
Title:	Teste_interno
Network:	Global Default Network
Asset Groups:	-
IPs:	192.168.50.42, 192.168.50.142
Excluded IPs:	-
Options Profile:	Initial Options

Summary of Vulnerabilities

Vulnerabilities Total	74

Security Risk (Avg)	4.5

by Severity

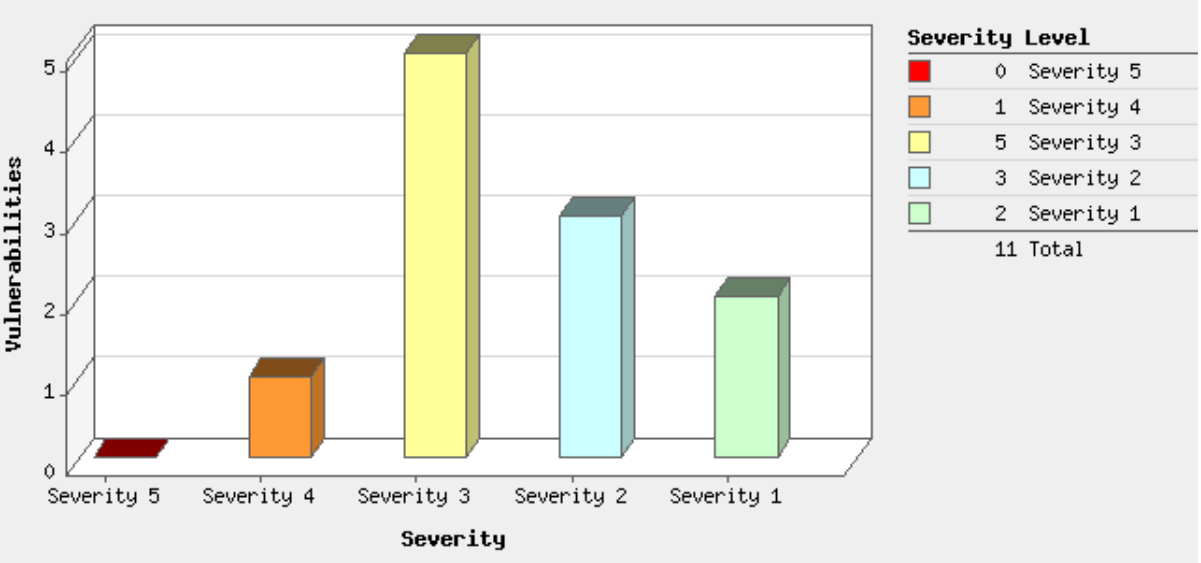
Severity	Confirmed	Potential	Information Gathered	Total
5	0	1	0	1
4	1	4	0	5
3	5	2	3	10
2	3	0	11	14
1	2	0	42	44
Total	11	7	56	74

5 Biggest Categories

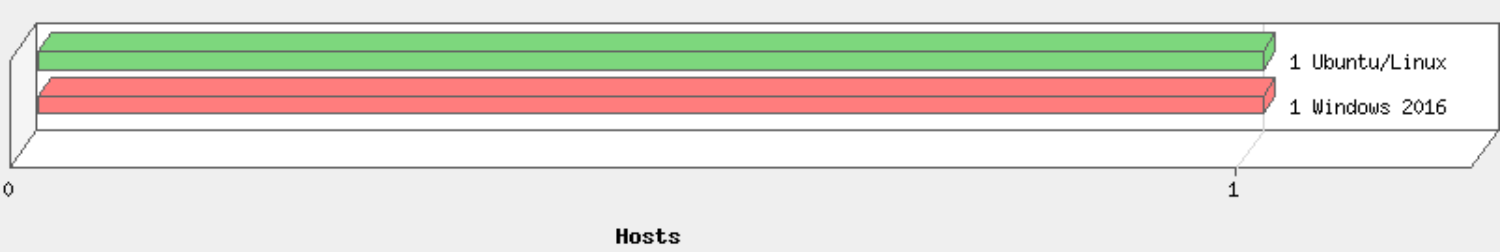
Category	Confirmed	Potential	Information Gathered	Total
Information gathering	0	0	26	26
CGI	3	3	8	14
TCP/IP	1	0	9	10
General remote services	6	0	3	9
Web server	0	1	5	6

Category	Confirmed	Potential	Information Gathered	Total
Total	10	4	51	65

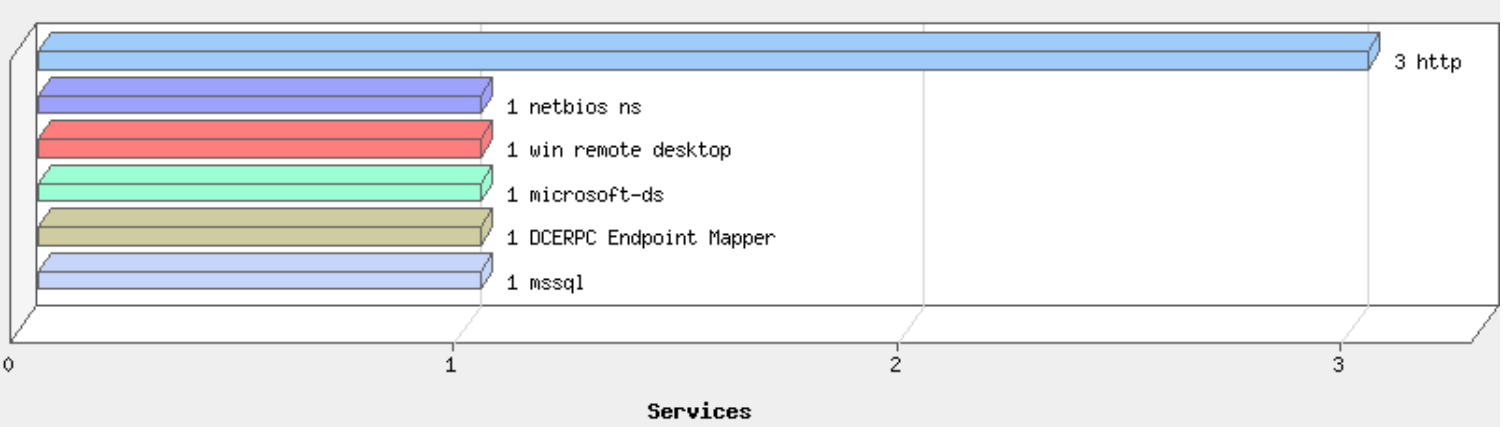
Vulnerabilities by Severity



Operating Systems Detected



Services Detected



Detailed Results

Vulnerabilities (8)

4 Microsoft SQL Server Elevation of Privilege Vulnerability - January 2021

QID:	91721
Category:	Windows
Associated CVEs:	CVE-2021-1636
Vendor Reference:	KB4583465, KB4583463, KB4583462, KB4583460, KB4583461, KB4583456, KB4583457, KB4583458, KB4583459
Bugtraq ID:	-
Service Modified:	05/31/2022
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
Microsoft SQL Server is prone to elevation of privilege vulnerability.

Affected Software:
SQL Server 2019 RTM (GDR,CU8)
SQL Server 2017 RTM (GDR,CU22)
SQL Server 2016 Service Pack 2(CU15,GDR)
SQL Server 2014 Service Pack 3 (GDR, CU4)
SQL Server 2012 Service Pack 4 (QFE)
QID Detection Logic (Authenticated):
Detection looks for Microsoft SQL Server instances and checks sqlservr.exe file version

IMPACT:
An authenticated attacker can send data over a network to an affected SQL Server when configured to run an Extended Event session.

SOLUTION:
Customers are advised to refer to CVE-2021-1636 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1636) for more details pertaining to this vulnerability.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Microsoft SQL Server(CVE-2021-1636) (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1636)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Vulnerable Version of Microsoft SQL Server detected on port 1433 - Microsoft SQL Server 11.00.7001 (MS SQL 2012)

3 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0) port 3389/tcp over SSL

QID:	38628
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	Deprecating TLS 1.0 and TLS 1.1
Bugtraq ID:	-
Service Modified:	07/12/2021
User Modified:	-
Edited:	No

PCI Vuln: Yes

THREAT:

TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs.
For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode.
RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack.
TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security.
A POODLE-type (https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls) attack could also be launched directly at TLS without negotiating a downgrade.
This QID is an automatic PCI FAIL in accordance with the PCI standards.
Further details can be found under:
PCI: ASV Program Guide v3.1 (page 27) (https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.1.pdf)
PCI: Use of SSL Early TLS and ASV Scans (https://www.pcisecuritystandards.org/documents/Use-of-SSL-Early-TLS-and-ASV-Scans.pdf)

NOTE: On March 31, 2021 Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) are formally deprecated.
Refer to Deprecating TLS 1.0 and TLS 1.1 (https://tools.ietf.org/html/rfc8996)

IMPACT:

An attacker can exploit cryptographic flaws to conduct man-in-the-middle type attacks or to decryption communications.
For example: An attacker could force a downgrade from the TLS protocol to the older SSLv3.0 protocol and exploit the POODLE vulnerability, read secure communications or maliciously modify messages.
A POODLE-type (https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls) attack could also be launched directly at TLS without negotiating a downgrade.

SOLUTION:

Disable the use of TLSv1.0 protocol in favor of a cryptographically stronger protocol such as TLSv1.2.
The following openssl commands can be used
to do a manual test:
openssl s_client -connect ip:port -tls1

If the test is successful, then the target support TLSv1

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.0 is supported

 3 SSLv3 Padding Oracle Attack Information Disclosure Vulnerability (POODLE) port 1433/tcp over SSL

QID:	38603
Category:	General remote services
Associated CVEs:	CVE-2014-3566
Vendor Reference:	POODLE
Bugtraq ID:	70574
Service Modified:	12/20/2018
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The SSL protocol 3.0 design error, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attacks.
The target supports SSLv3, which makes it vulnerable to POODLE (Padding Oracle On Downgraded Legacy Encryption), even if it also supports more recent versions of TLS. It's subject to a downgrade attack, in which the attacker tricks the browser into connecting with SSLv3.

This QID is an automatic PCI FAIL in accordance with the PCI standards.
Further details can be found under:
PCI: ASV Program Guide v3.1 (page 27) (https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.1.pdf)
PCI: Use of SSL Early TLS and ASV Scans (https://www.pcisecuritystandards.org/documents/Use-of-SSL-Early-TLS-and-ASV-Scans.pdf)

IMPACT:
An attacker who can take a man-in-the-middle (MitM) position can exploit this vulnerability and gain access to encrypted communication between a client and server.

SOLUTION:
Disable SSLv3 support to avoid this vulnerability.
Examples to disable SSLv3.
nginx: list specific allowed protocols in the "ssl_protocols" line. Make sure SSLv2 and SSLv3 is not listed. For example: ssl_protocols TLSv2 TLSv1.1 TLSv1.2;
Apache: Add -SSLv3 to the "SSLProtocol" line.
How to disable SSL 3.0 on Microsoft IIS (https://support.microsoft.com/kb/187498/en-us).
For PCI, please refer to the Qualys community article (https://community.qualys.com/thread/15280).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
Metasploit

Reference:	CVE-2014-3566
Description:	HTTP SSL/TLS Version Detection (POODLE scanner) - Metasploit Ref : /modules/auxiliary/scanner/http/ssl_version
Link:	https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/http/ssl_version.rb
Reference:	CVE-2014-3566
Description:	HTTP SSL/TLS Version Detection (POODLE scanner) - Metasploit Ref : /modules/auxiliary/scanner/http/axis_local_file_include
Link:	https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/http/ssl_version.rb
Reference:	CVE-2014-3566
Description:	HTTP SSL/TLS Version Detection (POODLE scanner) - Metasploit Ref : /modules/auxiliary/spoof/cisco/dtp
Link:	https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/http/ssl_version.rb

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
No results available

3 SSL Server Has SSLv3 Enabled Vulnerability — port 1433/tcp over SSL

QID:	38606
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/20/2018
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
SSL 3.0 is an obsolete and insecure protocol.
Encryption in SSL 3.0 uses either the RC4 stream cipher, or a block cipher in CBC mode.
RC4 is known to have biases, and the block cipher in CBC mode is vulnerable to the POODLE attack.
The SSLv3 protocol is insecure due to the POODLE attack and the weakness of RC4 cipher.
Note: In April 2016, PCI released PCI DSS v3.2 (https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf) announcing that NIST no longer considers Secure Socket Layers (SSL) v3.0 protocol as acceptable for protecting data and that all versions of SSL versions do not meet the PCI definition of "strong cryptography."

This QID is an automatic PCI FAIL in accordance with the PCI standards.
Further details can be found under:
PCI: ASV Program Guide v3.1 (page 27) (https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.1.pdf)
PCI: Use of SSL Early TLS and ASV Scans (https://www.pcisecuritystandards.org/documents/Use-of-SSL-Early-TLS-and-ASV-Scans.pdf)

IMPACT:
An attacker can exploit this vulnerability to read secure communications or maliciously modify messages.

SOLUTION:
Disable the SSL 3.0 protocol in the client and in the server, refer to
How to disable SSLv3 : Disable SSLv3 (http://disablessl3.com/)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
SSLv3 is supported

3 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0) port 1433/tcp over SSL

QID:	38628
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	Deprecating TLS 1.0 and TLS 1.1
Bugtraq ID:	-
Service Modified:	07/12/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs.
For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode.
RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack.
TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security.
A POODLE-type (https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls) attack could also be launched directly at TLS without negotiating a downgrade.
This QID is an automatic PCI FAIL in accordance with the PCI standards.
Further details can be found under:
PCI: ASV Program Guide v3.1 (page 27) (https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.1.pdf)
PCI: Use of SSL Early TLS and ASV Scans (https://www.pcisecuritystandards.org/documents/Use-of-SSL-Early-TLS-and-ASV-Scans.pdf)

NOTE: On March 31, 2021 Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) are formally deprecated.
Refer to Deprecating TLS 1.0 and TLS 1.1 (https://tools.ietf.org/html/rfc8996)

IMPACT:
An attacker can exploit cryptographic flaws to conduct man-in-the-middle type attacks or to decryption communications.
For example: An attacker could force a downgrade from the TLS protocol to the older SSLv3.0 protocol and exploit the POODLE vulnerability, read secure communications or maliciously modify messages.
A POODLE-type (https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls) attack could also be launched directly at TLS without negotiating a downgrade.

SOLUTION:
Disable the use of TLSv1.0 protocol in favor of a cryptographically stronger protocol such as TLSv1.2.
The following openssl commands can be used
to do a manual test:

openssl s_client -connect ip:port -tls1

If the test is successful, then the target support TLSv1

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLSv1.0 is supported

2 Microsoft ASP.NET Custom Errors Found Turned Off port 80/tcp

QID:	12034
Category:	CGI
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/10/2013
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
The "customErrors" tag in ASP.NET configuration files affects how error pages are managed in an ASP.NET application and whether developers can redirect users to their custom error pages when an exception is thrown.
ASP.NET produces an error page when an application throws an unhandled exception or when you deploy an .aspx file whose source contains a syntax error. Without custom errors, the error page generated might contain excerpts of the page's source code or stack traces, with confidential information not meant for remote clients.

IMPACT:
Sensitive information disclosed to remote clients may be used to launch future attacks. By redirecting the browser of the client to a sanitized custom error page, any such information leakage is avoided.

SOLUTION:
Use either the "On" or "RemoteOnly" configuration options for the "customErrors" attributes in the global machine.config or the installation-specific web.config file. Refer to ASP.NET Security (http://msdn.microsoft.com/en-us/library/91f66yxt(v=vs.100).aspx) on Microsoft MSDN for information on securing Web services.
Note that, we have found that ASP.NET 1.0 does not implement the customErrors modes properly, and even with a mode set to 'On' or 'RemoteOnly', the system may still generate exception messages from remoting requests. If the Results section below only shows the ".soap" remoting test, and not the ".asmx" web service test, then this is indeed the case. If possible, please upgrade to ASP.NET 1.1 framework. Else, if remoting is not being used, please disable the ".soap" handler using the IIS Configuration or the following configuration in the machine.config file:

```
<httpHandlers>
  <add verb="*" path="*.rem"
    type="System.Web.HttpForbiddenHandler"/>
  <add verb="*" path="*.soap"
    type="System.Web.HttpForbiddenHandler"/>
</httpHandlers>
```

If remoting is required, then ASP.NET version 1.1 provides a customErrors configuration for remoting specifically:

```
<configuration>
<system.runtime.remoting>
<customerrors mode="off"></customerrors>
</system.runtime.remoting>
</configuration>
```

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
System.Runtime.Remoting.RemotingException: Requested Service not found

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1) port 3389/tcp over SSL

QID:	38794
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	Deprecating TLS 1.0 and TLS 1.1
Bugtraq ID:	-
Service Modified:	07/12/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The scan target supports version 1.1 of the TLS protocol. That version is in the process of being deprecated and is no longer recommended. Instead the newer versions 1.2 and/or 1.3 should be used. The TLSv1.1 protocol itself does not have any currently exploitable vulnerabilities. However some vendor implementations of TLSv1.1 have weaknesses which may be exploitable.
This QID is posted as potential, when servers require client certificates and we cannot complete the handshake.
NOTE: On March 31, 2021 Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) are formally deprecated.
Refer to Deprecating TLS 1.0 and TLS 1.1 (https://tools.ietf.org/html/rfc8996)

IMPACT:
Supporting TLSv1.1 by itself does not necessarily have any harmful consequences, but it is no longer considered best practice because of bad past experience with some vendor implementations of TLSv1.1.

SOLUTION:
Disable the use of TLSv1.1 protocol in favor of a cryptographically stronger protocol such as TLSv1.2.
The following openssl commands can be used
to do a manual test:
openssl s_client -connect ip:port -tls1_1

If the test is successful, then the target support TLSv1.1

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLSv1.1 is supported

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1) port 1433/tcp over SSL

QID:	38794
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	Deprecating TLS 1.0 and TLS 1.1
Bugtraq ID:	-
Service Modified:	07/12/2021
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:

The scan target supports version 1.1 of the TLS protocol. That version is in the process of being deprecated and is no longer recommended. Instead the newer versions 1.2 and/or 1.3 should be used. The TLSv1.1 protocol itself does not have any currently exploitable vulnerabilities. However some vendor implementations of TLSv1.1 have weaknesses which may be exploitable.
This QID is posted as potential, when servers require client certificates and we cannot complete the handshake.
NOTE: On March 31, 2021 Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) are formally deprecated.
Refer to Deprecating TLS 1.0 and TLS 1.1 (https://tools.ietf.org/html/rfc8996)

IMPACT:

Supporting TLSv1.1 by itself does not necessarily have any harmful consequences, but it is no longer considered best practice because of bad past experience with some vendor implementations of TLSv1.1.

SOLUTION:

Disable the use of TLSv1.1 protocol in favor of a cryptographically stronger protocol such as TLSv1.2.
The following openssl commands can be used
to do a manual test:
openssl s_client -connect ip:port -tls1_1

If the test is successful, then the target support TLSv1.1

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.1 is supported

Potential Vulnerabilities (4)

5 EOL/Obsolete Software: Microsoft SQL Server 2012 Service Pack 4 (SP4) Detected

QID:	106085
Category:	Security Policy
Associated CVEs:	-
Vendor Reference:	Microsoft Product Lifecycle
Bugtraq ID:	-
Service Modified:	07/25/2022
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Microsoft SQL Server 2012 is a data management system that delivers a fixed set of features, data protection, and performance for embedded applications, lightweight Web Sites and applications, and local data stores.
Technical support and service pack support for the Service Pack 4 ended on Jul 12, 2022.
QID Detection Logic (Authenticated):
This QID looks for the registry keys and files to see if Microsoft SQL Server 2012 SP4 is installed or not.

IMPACT:

The system is at high risk of being exposed to security vulnerabilities. Since the vendor no longer provides updates, obsolete software is more prone to vulnerabilities.

SOLUTION:
Users are advised to obtain the SQL Server 2012 extended security update or SQL Server 2014 (https://www.microsoft.com/en-in/download/details.aspx?id=42299)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
EOL/Obsolete Software: Microsoft SQL Server 2012 Service Pack 4 (SP4) Detected on port 1433 \n - Microsoft SQL Server 11.00.7001 (MS SQL 2012)

4 Microsoft SQL Server Reporting Services Update for February 2020

QID:	91604
Category:	Windows
Associated CVEs:	CVE-2020-0618
Vendor Reference:	CVE-2020-0618
Bugtraq ID:	-
Service Modified:	04/04/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
A remote code execution vulnerability exists in Microsoft SQL Server Reporting Services when it incorrectly handles page requests. To exploit the vulnerability, an authenticated attacker would need to submit a specially crafted page request to an affected Reporting Services instance.
The security update addresses the vulnerability by modifying how the Microsoft SQL Server Reporting Services handles page requests.
Affected Software:
Microsoft SQL Server 2012 SP4
Microsoft SQL Server 2014 SP3
Microsoft SQL Server 2016 SP2
KBs targeted: 4532098, 4535288, 4532095, 4535706, 4532097.
QID Detection Logic:
This authenticated QID detects vulnerable file versions of the above mentioned software by:
Microsoft SQL Server 2016 SP2: fetching ReportServer\bin\ReportingServicesWebServer.dll from HKLM\SOFTWARE\Microsoft\Microsoft SQL Server\MSRS13.MSSQLSERVER\Setup\SQLPath and is lesser than 13.0.5102.14 or 13.0.5622.0.
Microsoft SQL Server 2014 SP3: fetching ReportServer\bin\Microsoft.ReportingServices.ProcessingObjectModel.dll from HKLM\SOFTWARE\Microsoft\Microsoft SQL Server\MSRS12.MSSQLSERVER\Setup\SQLPath and is lesser than 12.0.6118.4 or 12.0.6372.1.
Microsoft SQL Server 2012 SP4: fetching sqlservr.exe version from HKLM\SYSTEM\CurrentControlSet\Services and is lesser than 2011.110.7493.4.

IMPACT:
Successful exploitation allows an authenticated, remote attacker to execute code in the context of the Report Server service account.

SOLUTION:
Customers are advised to refer to CVE-2020-0618 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0618) for more details pertaining to this vulnerability.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
CVE-2020-0618 (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0618)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
Metasploit
Reference: CVE-2020-0618
Description: SQL Server Reporting Services (SSRS) ViewState Deserialization - Metasploit Ref : /modules/exploit/windows/http/

ssrs_navcorrector_viewstate

Link:
https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/http/ssrs_navcorrector_viewstate.rb

The Exploit-DB
Reference: CVE-2020-0618
Description: Microsoft SQL Server Reporting Services 2016 - Remote Code Execution - The Exploit-DB Ref : 48816
Link: http://www.exploit-db.com/exploits/48816

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
QID 91604 detected on port 1433 - Microsoft SQL Server 11.00.7001 (MS SQL 2012).

3 Microsoft SQL Server Database Link Crawling Command Execution - Zero Day

QID:	19824
Category:	Database
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/19/2017
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
Microsoft SQL Server is exposed to a remote command execution vulnerability.
Affected Versions:
Microsoft SQL Server 2005, 2008, 2008 R2, 2012 are affected.

IMPACT:
Successful exploitation could allow attackers to obtain sensitive information and execute arbitrary code.

SOLUTION:
There are no solutions available at this time.

Workaround:
Disable RPC_Out and xp_cmdshell for this issue.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
Qualys
Reference: CVE-0000-0000
Description: Microsoft SQL Server - Database Link Crawling Command Execution
Link: https://www.exploit-db.com/exploits/23649/

Reference: CVE-0000-0000
Description: Microsoft SQLServer - Database Link Crawling Command Execution
Link:
https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/windows/mssql/mssql_linkcrawler.rb

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:
QID 19824 detected on port 1433 - Microsoft SQL Server 11.00.7001 (MS SQL 2012)

3 Web Server Stopped Responding — port 80/tcp

QID:	86476
Category:	Web server
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/25/2022
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
The Web server stopped responding to 3 consecutive connection attempts and/or more than 3 consecutive HTTP / HTTPS requests. Consequently, the service aborted testing for HTTP / HTTPS vulnerabilities. The vulnerabilities already detected are still posted.

For more details about this QID, please review the following Qualys KB article:
(https://success.qualys.com/support/s/article/000003057#:~:text=The%20exhaustive%20Web%20Testing%20Skipped,network%20bandwidth%20is%20being%20overloaded)

IMPACT:
The service was unable to complete testing for HTTP / HTTPS vulnerabilities since the Web server stopped responding.

SOLUTION:
Check the Web server status.
If the Web server was crashed during the scan, please restart the server, report the incident to Customer Support and stop scanning the Web server until the issue is resolved.
If the Web server is unable to process multiple concurrent HTTP / HTTPS requests, please lower the scan harshness level and launch another scan.
If this vulnerability continues to be reported, please contact Customer Support.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
The web server did not respond for 4 consecutive HTTP requests.

After these, the service was still unable to connect to the web server 2 minutes later.

Information Gathered (27)

3 Remote Access or Management Service Detected

QID:	42017
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/02/2021
User Modified:	-
Edited:	No

PCI Vuln: No

THREAT:
A remote access or remote management service was detected. If such a service is accessible to malicious users it can be used to carry different type of attacks. Malicious users could try to brute force credentials or collect additional information on the service which could enable them in crafting further attacks.
The Results section includes information on the remote access service that was found on the target.
Services like Telnet, Rlogin, SSH, windows remote desktop, pcAnywhere, Citrix Management Console, Remote Admin (RAdmin), VNC, OPENVPN and ISAKMP are checked.

IMPACT:
Consequences vary by the type of attack.

SOLUTION:
Expose the remote access or remote management services only to the system administrators or intended users of the system.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Service name: Remote Desktop on TCP port 3389.

 2 Operating System Detected

QID:	45017
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/04/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.
1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.
Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.
2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).
3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.
4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:
Not applicable.

SOLUTION:

Not applicable.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Operating System	Technique	ID
Windows 2016	CIFS via TCP Port 445	
Windows 2016/2019/10	NTLMSSP	
Windows Vista / Windows 2008 / Windows 7 / Windows 2012 / Windows 8 / Windows 10	TCP/IP Fingerprint	U3414:80
Windows 2003/XP/Vista/2008/2012	MS-RPC Fingerprint	

2 Open DCE-RPC / MS-RPC Services List

QID:	70022
Category:	SMB / NETBIOS
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/22/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following DCE-RPC / MS-RPC services are active on the remote host.

IMPACT:
N/A

SOLUTION:
Shut down any unknown or unused service on the list. In Windows, this is done in the "Services" Control Panel. In other environments, this usually requires editing a configuration file or start-up script.

If you have provided Windows Authentication credentials, the Microsoft
Registry service supporting the named pipe "\PIPE\winreg" must be present to allow CIFS to access the Registry.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Description	Version	TCP Ports	UDP Ports	HTTP Ports	NetBIOS/CIFS Pipes
DCE Endpoint Mapper	3.0	135			
DCOM OXID Resolver	0.0	135			
DCOM Remote Activation	0.0	135			
DCOM System Activator	0.0	135			
Microsoft Scheduler Control Service	1.0				\PIPE\atsvc, \pipe\SessEnvPublicRpc
Microsoft Security Account Manager	1.0	49681			\pipe\lsass

Microsoft Service Control Service	2.0	49669	
Microsoft Spool Subsystem	1.0	49667	
Microsoft Task Scheduler	1.0		\PIPE\atsvc, \pipe\SessEnvPublicRpc
(Unknown Service)	1.0	135	
(Unknown Service)	0.0	135	
(Unknown Service)	2.0	135	
(Unknown Service)	1.0	49664	\PIPE\InitShutdown
(Unknown Service)	1.0		\PIPE\InitShutdown
(Unknown Service)	1.0		\pipe\LSM_API_service
(Unknown Service)	1.0	49665, 49666	\pipe\LSM_API_service, \pipe\eventlog, \PIPE\atsvc, \pipe\SessEnvPublicRpc
(Unknown Service)	0.0		\pipe\LSM_API_service
(Unknown Service)	1.0	49665	\pipe\eventlog
DHCP Client LRPC Endpoint	1.0	49665	\pipe\eventlog
DHCPv6 Client LRPC Endpoint	1.0	49665	\pipe\eventlog
Event log TCPIP	1.0	49665	\pipe\eventlog
Adh APIs	1.0	49666	\PIPE\atsvc, \pipe\SessEnvPublicRpc
Proxy Manager client server endpoint	1.0	49666	\PIPE\atsvc, \pipe\SessEnvPublicRpc
Proxy Manager provider server endpoint	1.0	49666	\PIPE\atsvc, \pipe\SessEnvPublicRpc
IP Transition Configuration endpoint	1.0	49666	\PIPE\atsvc, \pipe\SessEnvPublicRpc
UserMgrCli	1.0	49666	\PIPE\atsvc, \pipe\SessEnvPublicRpc
IKE/Authip API	1.0	49666	\PIPE\atsvc, \pipe\SessEnvPublicRpc
(Unknown Service)	1.0	49666	\PIPE\atsvc, \pipe\SessEnvPublicRpc
(Unknown Service)	2.0	49666	\PIPE\atsvc, \pipe\SessEnvPublicRpc
DfsDs service	1.0		\PIPE\wkssvc
(Unknown Service)	1.0	49667	
Remote Fw APIs	1.0	49668	
Ngc Pop Key Service	1.0		\pipe\lsass
KeyIso	2.0		\pipe\lsass

 2 Microsoft SQL Server Version Information Gathered

QID:	90087
Category:	Windows
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/20/2014
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The scanner probed the target host's Windows Registry or the SQL TCP port, and has gathered the version information for the Microsoft SQL Server installed on the target host.
The version information is shown in the Results section. "CurrentVersion" gives the version of the original Microsoft SQL Server installation on the target host. "CSDVersion", if present, gives the updated version due to any later patches/service packs installed on the host. The version obtained from the TCP port (typically 1433) is listed separately as well (if found).
Though the registry value and the one got from TDS protocol are reliable to a good degree in identifying the patch levels like service packs and cumulative patches, they may not reflect version changes due to all hotfixes.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
QID 90087 detected on port 1433 - Microsoft SQL Server 11.00.7001 (MS SQL 2012)

2 Windows Registry Pipe Access Level

QID:	90194
Category:	Windows
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/16/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Return code from remote access to the Windows registry pipe is displayed. The CIFS service accesses the Windows registry through a named pipe. Authentication to CIFS was successful, but it could not access the Registry named pipe if the error code is not 0.

IMPACT:
Vulnerabilities that require Windows registry access may not have been detected during the scan if the error code is not 0.

SOLUTION:
Error code 0x00 means the pipe access was successful. Other error codes (for eg: 0x0) denote unsuccessful access.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Access to Remote Registry Service is denied, error: 0x0

2 Microsoft ASP.NET HTTP Handlers Enumerated port 80/tcp

QID:	12033
Category:	CGI
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/25/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Microsoft ASP.NET HTTP handlers are used for processing Web requests for specific file extensions. For example, .aspx is used for ASP.NET pages, .rem and .soap are used for remoting, .asmx is used for Web services. These extensions are located in the "machine.config" file under the "httpHandlers" element.
The scanner enummerated the common HTTP handlers present on the target ASP.NET system, and these handlers are displayed in the Results section below.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
.Aspx,.Asmx,.Rem,.Soap,

2 Microsoft IIS ISAPI Application Filters Mapped To Home Directory port 80/tcp

QID:	12049
Category:	CGI
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/04/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The scanner enumerated the ISAPI filters mapped to the target Microsoft Internet Information Services (IIS) Web server's home directory "/". These are listed in the Result section below.

IMPACT:
Most of the ISAPI filters come by default with IIS, and typically most of them are never used in Web applications. Further, there have been quite a few buffer overflow based remote code execution or denial of service attacks reported for many of these ISAPI filters.

SOLUTION:
Disable the ISAPI filters not being used on the target. This can be done using the "Internet Information Services" MMC snap-in's "Home Directory" section (under "Configuration").
Microsoft provides a free tool named LockDown to secure IIS. LockDown is available at : http://www.microsoft.com/technet/security/tools/locktool.mspx (http://www.microsoft.com/technet/security/tools/locktool.mspx).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
.Aspx,.Asmx,.Rem,.Soap,

2 Web Server HTTP Protocol Versions port 80/tcp

QID:	45266
Category:	Information gathering
Associated CVEs:	-

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Remote Web Server supports HTTP version 1.x on 80 port.GET / HTTP/1.1

1 DNS Host Name

QID:	6
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
192.168.50.42	win-nhkro5kp3fn

1 Host Scan Time - Scanner

QID:	45038
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/16/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Scan duration: 2073 seconds

Start time: Mon, Aug 01 2022, 18:22:05 GMT

End time: Mon, Aug 01 2022, 18:56:38 GMT

1 Host Names Found

QID:	45039
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/27/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
WIN-NHKRO5KP3FN	NTLM DNS
win-nhkro5kp3fn	FQDN
WIN-NHKRO5KP3FN	NTLM NetBIOS

 1 Scan Activity per Port

QID:	45426
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	80	1:49:33
TCP	135	0:00:40
TCP	445	0:00:04
TCP	1433	0:06:10
TCP	3389	0:05:34
UDP	123	0:00:19
UDP	137	0:00:25
UDP	138	0:00:07
UDP	500	0:00:12
UDP	1900	0:00:12

 1 Microsoft Server Message Block (SMBv3) Compression Disabled

QID:	48086
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/13/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The remote host supports Microsoft Server Message Block 3.1.1 (SMBv3) protocol with compression feature disabled.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Microsoft Server Message Block (SMBv3) Compression Disabled

 1 Windows Authentication Method

QID:	70028
Category:	SMB / NETBIOS
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/09/2008
User Modified:	-
Edited:	No

PCI Vuln: No

THREAT:
Windows authentication was performed. The Results section in your detailed results includes a list of authentication credentials used.
The service also attempts to authenticate using common credentials. You should verify that the credentials used for successful authentication were those that were provided in the Windows authentication record. User-provided credentials failed if the discovery method shows "Unable to log in using credentials provided by user, fallback to NULL session". If this is the case, verify that the credentials specified in the Windows authentication record are valid for this host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

User Name	(none)
Domain	(none)
Authentication Scheme	NULL session
Security	User-based
SMBv1 Signing	Disabled
Discovery Method	NULL session, no valid login credentials provided or found
CIFS Signing	default

 1 File and Print Services Access Denied

QID: 70038
Category: SMB / NETBIOS
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 06/06/2005
User Modified: -
Edited: No
PCI Vuln: No

THREAT:
Remote Access to File and Print Services did not succeed. This is provided by Common Internet File System (CIFS) service. If you provided Windows
Authentication credentials, the Windows Authentication Method QID or the Windows Authentication Failed QID will not be reported if this service is not running.

IMPACT:
Vulnerabilities that require authenticated access may not be reported.

SOLUTION:
On a Windows host, make sure that the network setting for File and Print Services is enabled and the "Server" service (CIFS) is running.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
No results available

1 Open UDP Services List

QID:	82004
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/11/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.
Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected
123	ntp	Network Time Protocol	unknown
137	netbios-ns	NETBIOS Name Service	netbios ns
138	netbios-dgm	NETBIOS Datagram Service	unknown
500	isakmp	isakmp	unknown
1900	unknown	unknown	unknown

1 Open TCP Services List

QID:	82023
Category:	TCP/IP
Associated CVEs:	-

Vendor Reference: -
Bugtraq ID: -
Service Modified: 06/15/2009
User Modified: -
Edited: No
PCI Vuln: No

THREAT:
The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
80	www-http	World Wide Web HTTP	http	
135	msrpc-epmap	epmap DCE endpoint resolution	DCERPC Endpoint Mapper	
445	microsoft-ds	Microsoft-DS	microsoft-ds	
1433	ms-sql-s	Microsoft-SQL-Server	mssql	
3389	ms-wbt-server	MS WBT Server	win remote desktop	


1 ICMP Replies Received

QID: 82040
Category: TCP/IP
Associated CVEs: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 01/16/2003
User Modified: -
Edited: No
PCI Vuln: No

THREAT:
ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)

IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Time Stamp (type=14 code=0)	Time Stamp Request	18:22:52 GMT
Unreachable (type=3 code=3)	UDP Port 1	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 456	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1245	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 7	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 40412	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 2115	Port Unreachable
Unreachable (type=3 code=2)	IP with High Protocol	Protocol Unreachable
Unreachable (type=3 code=3)	UDP Port 121	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 3391	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 3129	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 7306	Port Unreachable

1 NetBIOS Host Name

QID:	82044
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/20/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The NetBIOS host name of this computer has been detected.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
WIN-NHKRO5KP3FN

1 Default Web Page port 80/tcp

QID:	12230
Category:	CGI
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/16/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
GET / HTTP/1.0
Host: win-nhkro5kp3fn

HTTP/1.1 403 Forbidden
Content-Type: text/html
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Mon, 01 Aug 2022 18:23:54 GMT
Connection: keep-alive
Content-Length: 1233

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>403 - Forbidden: Access is denied.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->

```
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
 <div class="content-container"><fieldset>
  <h2>403 - Forbidden: Access is denied.</h2>
  <h3>You do not have permission to view this directory or page using the credentials that you supplied.</h3>
 </fieldset></div>
</div>
</body>
</html>
```

1 Default Web Page (Follow HTTP Redirection) port 80/tcp

QID:	13910
Category:	CGI
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: win-nhkro5kp3fn


HTTP/1.1 403 Forbidden
Content-Type: text/html
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Mon, 01 Aug 2022 18:25:14 GMT
Connection: keep-alive
Content-Length: 1233

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>403 - Forbidden: Access is denied.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
```

```
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
 <div class="content-container"><fieldset>
  <h2>403 - Forbidden: Access is denied.</h2>
  <h3>You do not have permission to view this directory or page using the credentials that you supplied.</h3>
 </fieldset></div>
</div>
</body>
</html>
```

1 HTTP Methods Returned by OPTIONS Request port 80/tcp

QID:	45056
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Allow: OPTIONS, TRACE, GET, HEAD, POST

1 HTTP Response Method and Header Information Collected port 80/tcp

QID:	48118
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No

PCI Vuln: No

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
HTTP header and method information collected on port 80.

GET / HTTP/1.0
Host: win-nhkro5kp3fn

HTTP/1.1 403 Forbidden
Content-Type: text/html
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Mon, 01 Aug 2022 18:23:54 GMT
Connection: keep-alive
Content-Length: 1233

 1 Microsoft IIS ASP.NET Version Obtained port 80/tcp

QID:	86484
Category:	Web server
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/25/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The ASP.NET version running on the Microsoft IIS Server has been retrieved.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.6.1586.0

1 List of Web Directories port 80/tcp

QID:	86672
Category:	Web server
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/aspnet_client/	brute force

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance port 3389/tcp over SSL

QID:	38597
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	rejected
0399	rejected
0400	rejected
0499	rejected

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance port 1433/tcp over SSL

QID:	38597
Category:	General remote services
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	rejected
0399	rejected
0400	rejected
0499	rejected

Vulnerabilities (3)

3 TCP Sequence Number Approximation Based Denial of Service

QID:	82054
Category:	TCP/IP
Associated CVEs:	CVE-2004-0230
Vendor Reference:	-
Bugtraq ID:	10183
Service Modified:	05/04/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

TCP provides stateful communications between hosts on a network. TCP sessions are established by a three-way handshake and use random 32-bit sequence and acknowledgement numbers to ensure the validity of traffic. A vulnerability was reported that may permit TCP sequence numbers to be more easily approximated by remote attackers. This issue affects products released by multiple vendors.
The cause of the vulnerability is that affected implementations will accept TCP sequence numbers within a certain range, known as the acknowledgement range, of the expected sequence number for a packet in the session. This is determined by the TCP window size, which is negotiated during the three-way handshake for the session. Larger TCP window sizes may be set to allow for more throughput, but the larger the TCP window size, the more probable it is to guess a TCP sequence number that falls within an acceptable range. It was initially thought that guessing an acceptable sequence number was relatively difficult for most implementations given random distribution, making this type of attack impractical. However, some implementations may make it easier to successfully approximate an acceptable TCP sequence number, making these attacks possible with a number of protocols and implementations.
This is further compounded by the fact that some implementations may support the use of the TCP Window Scale Option, as described in RFC 1323, to extend the TCP window size to a maximum value of 1 billion.
This vulnerability will permit a remote attacker to inject a SYN or RST packet into the session, causing it to be reset and effectively allowing for denial of service attacks. An attacker would exploit this issue by sending a packet to a receiving implementation with an approximated sequence number and a forged source IP address and TCP port.
There are a few factors that may present viable target implementations, such as those which depend on long-lived TCP connections, those that have known or easily guessed IP address endpoints and those implementations with easily guessed TCP source ports. It has been noted that Border Gateway Protocol (BGP) is reported to be particularly vulnerable to this type of attack, due to the use of long-lived TCP sessions and the possibility that some implementations may use the TCP Window Scale Option. As a result, this issue is likely to affect a number of routing platforms.
Another factor to consider is the relative difficulty of injecting packets into TCP sessions, as a number of receiving implementations will reassemble packets in order, dropping any duplicates. This may make some implementations more resistant to attacks than others.
It should be noted that while a number of vendors have confirmed this issue in various products, investigations are ongoing and it is likely that many other vendors and products will turn out to be vulnerable as the issue is investigated further.

IMPACT:

Successful exploitation of this issue could lead to denial of service attacks on the TCP based services of target hosts.

SOLUTION:

Please first check the results section below for the port number on which this vulnerability was detected. If that port number is known to be used for port-forwarding, then it is the backend host that is really vulnerable.
Various implementations and products including Check Point, Cisco, Cray Inc, Hitachi, Internet Initiative Japan, Inc (IIJ), Juniper Networks, NEC, Polycom, and Yamaha are currently undergoing review. Contact the vendors to obtain more information about affected products and fixes. NISCC Advisory 236929 - Vulnerability Issues in TCP (http://packetstormsecurity.org/0404-advisories/246929.html) details the vendor patch status as of the time of the advisory, and identifies resolutions and workarounds.
Refer to US-CERT Vulnerability Note VU#415294 (http://www.kb.cert.org/vuls/id/415294) and OSVDB Article 4030 (http://osvdb.org/4030) to obtain a list of vendors affected by this issue and a note on resolutions (if any) provided by the vendor.
For Microsoft: Refer to MS05-019 (https://docs.microsoft.com/en-us/security-updates/securitybulletins/2005/ms05-019) and MS06-064 (https://docs.microsoft.com/en-us/security-updates/securitybulletins/2006/ms06-064) for further details.
For SGI IRIX: Refer to SGI Security Advisory 20040905-01-P (ftp://patches.sgi.com/support/free/security/advisories/20040905-01-P.asc)
For SCO UnixWare 7.1.3 and 7.1.1: Refer to SCO Security Advisory SCOSA-2005.14 (ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.14/SCOSA-2005.14.txt)
For Solaris (Sun Microsystems): The vendor has acknowledged the vulnerability; however a patch is not available. Refer to Sun Microsystems, Inc. Information for VU#415294 (http://www.kb.cert.org/vuls/id/JARL-5YGQAJ) to obtain additional details. Also, refer to TA04-111A (http://www.us-cert.gov/cas/techalerts/TA04-111A.html) for detailed mitigating strategies against these attacks.
For NetBSD: Refer to NetBSD-SA2004-006 (ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc)
For Cisco: Refer to cisco-sa-20040420-tcp-ios.shtml (http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml).
For IBM : Refer to IBM-tcp-sequence-number-cve-2004-0230 (https://www.ibm.com/support/pages/tcp-sequence-number-approximation-based-denial-service-cve-2004-0230).
For Red Hat Linux: There is no fix available.
Workaround:The following BGP-specific workaround information has been provided.

For BGP implementations that support it, the TCP MD5 Signature Option should be enabled. Passwords that the MD5 checksum is applied to should be set to strong values and changed on a regular basis.
Secure BGP configuration instructions have been provided for Cisco and Juniper at these locations:

Secure Cisco IOS BGP Template (http://www.cymru.com/Documents/secure-bgp-template.html)

JUNOS Secure BGP Template (http://www.cymru.com/gillsr/documents/junos-bgp-template.pdf)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
The Exploit-DB

Reference:	CVE-2004-0230
Description:	Microsoft Windows - Malformed IP Options Denial of Service (MS05-019) - The Exploit-DB Ref : 942
Link:	http://www.exploit-db.com/exploits/942
Reference:	CVE-2004-0230
Description:	Microsoft Windows XP/2000 - TCP Connection Reset - The Exploit-DB Ref : 276
Link:	http://www.exploit-db.com/exploits/276
Reference:	CVE-2004-0230
Description:	TCP Connection Reset - Remote Denial of Service - The Exploit-DB Ref : 291
Link:	http://www.exploit-db.com/exploits/291
Reference:	CVE-2004-0230
Description:	Multiple Vendor - TCP Sequence Number Approximation (1) - The Exploit-DB Ref : 24030
Link:	http://www.exploit-db.com/exploits/24030
Reference:	CVE-2004-0230
Description:	Multiple Vendor - TCP Sequence Number Approximation (2) - The Exploit-DB Ref : 24031
Link:	http://www.exploit-db.com/exploits/24031
Reference:	CVE-2004-0230
Description:	Multiple Vendor - TCP Sequence Number Approximation (3) - The Exploit-DB Ref : 24032
Link:	http://www.exploit-db.com/exploits/24032
Reference:	CVE-2004-0230
Description:	Multiple Vendor - TCP Sequence Number Approximation (4) - The Exploit-DB Ref : 24033
Link:	http://www.exploit-db.com/exploits/24033

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Tested on port 80 with an injected SYN/RST offset by 16 bytes.

2 HTTP Security Header Not Detected — port 80/tcp

QID:	11827
Category:	CGI
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/27/2022
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
This QID reports the absence of the following HTTP headers (https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#tab=Headers)

according to CWE-693: Protection Mechanism Failure (https://cwe.mitre.org/data/definitions/693.html):

X-Content-Type-Options: This HTTP header will prevent the browser from interpreting files as a different MIME type to what is specified in the Content-Type HTTP header.
Strict-Transport-Security: The HTTP Strict-Transport-Security response header (HSTS) allows web servers to declare that web browsers (or other complying user agents) should only interact with it using secure HTTPS connections, and never via the insecure HTTP protocol.

QID Detection Logic:
This unauthenticated QID looks for the presence of the following HTTP responses:
The Valid directives are as belows:
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=< [;includeSubDomains]

IMPACT:

Depending on the vulnerability being exploited, an unauthenticated remote attacker could conduct cross-site scripting, clickjacking or MIME-type sniffing attacks.

SOLUTION:

Note: To better debug the results of this QID, it is requested that customers execute commands to simulate the following functionality: curl -lkL --verbose.
CWE-693: Protection Mechanism Failure mentions the following - The product does not use or incorrectly uses a protection mechanism that provides sufficient defense against directed attacks against the product. A "missing" protection mechanism occurs when the application does not define any mechanism against a certain class of attack. An "insufficient" protection mechanism might provide some defenses - for example, against the most common attacks - but it does not protect against everything that is intended. Finally, an "ignored" mechanism occurs when a mechanism is available and in active use within the product, but the developer has not applied it in some code path.
Customers are advised to set proper X-Content-Type-Options (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options) and Strict-Transport-Security (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security) HTTP response headers.
Depending on their server software, customers can set directives in their site configuration or Web.config files. Few examples are:
X-Content-Type-Options:
Apache: Header always set X-Content-Type-Options: nosniff
HTTP Strict-Transport-Security:
Apache: Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"
Nginx: add_header Strict-Transport-Security max-age=31536000;
Note: Network devices that include a HTTP/HTTPS console for administrative/management purposes often do not include all/some of the security headers. This is a known issue and it is recommend to contact the vendor for a solution.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

X-Content-Type-Options HTTP Header missing on port 80.

GET / HTTP/1.0
Host: kali

HTTP/1.1 200 OK
Date: Mon, 01 Aug 2022 18:36:41 GMT
Server: Apache/2.4.51 (Debian)
Last-Modified: Mon, 20 Dec 2021 06:27:35 GMT
ETag: "29cd-5d38dfc099e6d"
Accept-Ranges: bytes
Content-Length: 10701
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

 2 HTTP Security Header Not Detected port 8000/tcp

QID: 11827
Category: CGI

Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/27/2022
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

This QID reports the absence of the following HTTP headers (https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#tab=Headers) according to CWE-693: Protection Mechanism Failure (https://cwe.mitre.org/data/definitions/693.html):

X-Content-Type-Options: This HTTP header will prevent the browser from interpreting files as a different MIME type to what is specified in the Content-Type HTTP header.
Strict-Transport-Security: The HTTP Strict-Transport-Security response header (HSTS) allows web servers to declare that web browsers (or other complying user agents) should only interact with it using secure HTTPS connections, and never via the insecure HTTP protocol.

QID Detection Logic:
This unauthenticated QID looks for the presence of the following HTTP responses:
The Valid directives are as belows:
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=< [;includeSubDomains]

IMPACT:

Depending on the vulnerability being exploited, an unauthenticated remote attacker could conduct cross-site scripting, clickjacking or MIME-type sniffing attacks.

SOLUTION:

Note: To better debug the results of this QID, it is requested that customers execute commands to simulate the following functionality: curl -IkL --verbose.
CWE-693: Protection Mechanism Failure mentions the following - The product does not use or incorrectly uses a protection mechanism that provides sufficient defense against directed attacks against the product. A "missing" protection mechanism occurs when the application does not define any mechanism against a certain class of attack. An "insufficient" protection mechanism might provide some defenses - for example, against the most common attacks - but it does not protect against everything that is intended. Finally, an "ignored" mechanism occurs when a mechanism is available and in active use within the product, but the developer has not applied it in some code path.
Customers are advised to set proper X-Content-Type-Options (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options) and Strict-Transport-Security (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security) HTTP response headers.
Depending on their server software, customers can set directives in their site configuration or Web.config files. Few examples are:
X-Content-Type-Options:
Apache: Header always set X-Content-Type-Options: nosniff
HTTP Strict-Transport-Security:
Apache: Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"
Nginx: add_header Strict-Transport-Security max-age=31536000;
Note: Network devices that include a HTTP/HTTPS console for administrative/management purposes often do not include all/some of the security headers. This is a known issue and it is recommend to contact the vendor for a solution.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

X-Content-Type-Options HTTP Header missing on port 8000.

GET / HTTP/1.0
Host: kali:8000

HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/3.9.8

Date: Mon, 01 Aug 2022 18:24:40 GMT
Content-type: text/html; charset=utf-8
Content-Length: 297

Potential Vulnerabilities (3)

4 Apache Hypertext Transfer Protocol (HTTP) Server Buffer Overflow Vulnerability port 80/tcp

QID:	730312
Category:	CGI
Associated CVEs:	CVE-2021-44790
Vendor Reference:	Apache HTTP Server Security Advisory
Bugtraq ID:	-
Service Modified:	12/23/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
Apache HTTP Server is a free and open-source cross-platform web server software, released under the terms of Apache License 2.0.
A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts).
Affected Versions:
Apache HTTP Server 2.4.51 and earlier
QID Detection Logic:(Unauthenticated)
This QID checks for vulnerable Apache Version by grabbing the banner from HTTP response

IMPACT:

Successful exploitation of the vulnerability may allow remote code execution and complete system compromise.

SOLUTION:
Customers are advised to update to Apache HTTP Server 2.4.52 or later. For more information, check Apache Security Advisory (https://httpd.apache.org/security/vulnerabilities_24.html)

Patch:
Following are links for downloading patches to fix the vulnerabilities:
Apache Security Advisory (https://httpd.apache.org/security/vulnerabilities_24.html)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Vulnerable Apache HTTP Server detected on port 80 -
Date: Mon, 01 Aug 2022 18:23:13 GMT
Server: Apache/2.4.51 (Debian)
Last-Modified: Mon, 20 Dec 2021 06:27:35 GMT
ETag: "29cd-5d38dfc099e6d"
Accept-Ranges: bytes
Content-Length: 10701
Vary: Accept-Encoding
Connection: close
Content-Type: text/html

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Apache2 Debian Default Page: It works</title>
```

```
    <style type="text/css" media="screen">
  * {
    margin: 0px 0px 0px 0px;
    padding: 0px 0px 0px 0px;
  }

  body, html {
    padding: 3px 3px 3px 3px;

    background-color: #D8DBE2;

    font-family: Verdana, sans-serif;
    font-size: 11pt;
    text-align: center;
  }

  div.main_page {
    position: relative;
    display: table;

    width: 800px;

    margin-bottom: 3px;
    margin-left: auto;
    margin-right: auto;
    paddinGET / HTTP/1.0
Host: kali
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:60.0) Gecko/20100101 Firefox/60.0



Vulnerable Version of Apache HTTP Server Detected on port: 80
HTTP/1.1 200 OK
Date: Mon, 01 Aug 2022 18:40:16 GMT
Server: Apache/2.4.51 (Debian)
Last-Modified: Mon, 20 Dec 2021 06:27:35 GMT
ETag: "29cd-5d38dfc099e6d"
Accept-Ranges: bytes
Content-Length: 10701
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Apache2 Debian Default Page: It works</title>
    <style type="text/css" media="screen">
  * {
    margin: 0px 0px 0px 0px;
    padding: 0px 0px 0px 0px;
  }

  body, html {
    padding: 3px 3px 3px 3px;

    background-color: #D8DBE2;

    font-family: Verdana, sans-serif;
    font-size: 11pt;
    text-align: center;
  }

  div.main_page {
    position: relative;
    display: table;

    width: 800px;

    margin-bottom: 3px;
    margin-left: auto;
    margin-right: auto;
    padding: 0px 0px 0px 0px;

    border-width: 2px;
```

```
  border-color: #212738;
  border-style: solid;

  background-color: #FFFFFF;

  text-align: center;
}

div.page_header {
  height: 99px;
  width: 100%;

  background-color: #F5F6F7;
}

div.page_header span {
  margin: 15px 0px 0px 50px;

  font-size: 180%;
  font-weight: bold;
}

div.page_header img {
  margin: 3px 0px 0px 40px;

  border: 0px 0px 0px;
}

div.table_of_contents {
  clear: left;

  min-width: 200px;

  margin: 3px 3px 3px 3px;

  background-color: #FFFFFF;

  text-align: left;
}

div.table_of_contents_item {
  clear: left;

  width: 100%;

  margin: 4px 0px 0px 0px;

  background-color: #FFFFFF;

  color: #000000;
  text-align: left;
}

div.table_of_contents_item a {
  margin: 6px 0px 0px 6px;
}

div.content_section {
  margin: 3px 3px 3px 3px;

  background-color: #FFFFFF;

  text-align: left;
}

div.content_section_text {
  padding: 4px 8px 4px 8px;

  color: #000000;
  font-size: 100%;
}

div.content_section_text pre {
  margin: 8px 0px 8px 0px;
  padding: 8px 8px 8px 8px;

  border-width: 1px;
  border-style: dotted;
```

```
  border-color: #000000;

  background-color: #F5F6F7;

  font-style: italic;
}

div.content_section_text p {
  margin-bottom: 6px;
}

div.content_section_text ul, div.content_section_text li {
  padding: 4px 8px 4px 16px;
}

div.section_header {
  padding: 3px 6px 3px 6px;

  background-color: #8E9CB2;

  color: #FFFFFF;
  font-weight: bold;
  font-size: 112%;
  text-align: center;
}

div.section_header_red {
  background-color: #CD214F;
}

div.section_header_grey {
  background-color: #9F9386;
}

.floating_element {
  position: relative;
  float: left;
}

div.table_of_contents_item a,
div.content_section_text a {
  text-decoration: none;
  font-weight: bold;
}

div.table_of_contents_item a:link,
div.table_of_contents_item a:visited,
div.table_of_contents_item a:active {
  color: #000000;
}

div.table_of_contents_item a:hover {
  background-color: #000000;

  color: #FFFFFF;
}

div.content_section_text a:link,
div.content_section_text a:visited,
 div.content_section_text a:active {
  background-color: #DCDFE6;

  color: #000000;
}

div.content_section_text a:hover {
  background-color: #000000;

  color: #DCDFE6;
}

div.validator {
}
  </style>
</head>
<body>
  <div class="main_page">
    <div class="page_header floating_element">
```

```
      <img src="/icons/openlogo-75.png" alt="Debian Logo" class="floating_element"/>
      <span class="floating_element">
        Apache2 Debian Default Page
      </span>
    </div>
<!--      <div class="table_of_contents floating_element">
      <div class="section_header section_header_grey">
        TABLE OF CONTENTS
      </div>
      <div class="table_of_contents_item floating_element">
        <a href="#about">About</a>
      </div>
      <div class="table_of_contents_item floating_element">
        <a href="#changes">Changes</a>
      </div>
      <div class="table_of_contents_item floating_element">
        <a href="#scope">Scope</a>
      </div>
      <div class="table_of_contents_item floating_element">
        <a href="#files">Config files</a>
      </div>
    </div>
-->
    <div class="content_section floating_element">


      <div class="section_header section_header_red">
        <div id="about"></div>
        It works!
      </div>
      <div class="content_section_text">
        <p>
            This is the default welcome page used to test the correct
            operation of the Apache2 server after installation on Debian systems.
            If you can read this page, it means that the Apache HTTP server installed at
            this site is working properly. You should <b>replace this file</b> (located at
            <tt>/var/www/html/index.html</tt>) before continuing to operate your HTTP server.
        </p>


        <p>
            If you are a normal user of this web site and don't know what this page is
            about, this probably means that the site is currently unavailable due to
            maintenance.
            If the problem persists, please contact the site's administrator.
        </p>

      </div>
      <div class="section_header">
        <div id="changes"></div>
            Configuration Overview
      </div>
      <div class="content_section_text">
        <p>
            Debian's Apache2 default configuration is different from the
            upstream default configuration, and split into several files optimized for
            interaction with Debian tools. The configuration system is
            <b>fully documented in
            /usr/share/doc/apache2/README.Debian.gz</b>. Refer to this for the full
            documentation. Documentation for the web server itself can be
            found by accessing the <a href="/manual">manual</a> if the <tt>apache2-doc</tt>
            package was installed on this server.

        </p>
        <p>
            The configuration layout for an Apache2 web server installation on Debian systems is as follows:
        </p>
        <pre>
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

```
 </pre>
 <ul>
          <li>
            <tt>apache2.conf</tt> is the main configuration
            file. It puts the pieces together by including all remaining configuration
            files when starting up the web server.
          </li>

          <li>
            <tt>ports.conf</tt> is always included from the
            main configuration file. It is used to determine the listening ports for
            incoming connections, and this file can be customized anytime.
          </li>

          <li>
            Configuration files in the <tt>mods-enabled/</tt>,
            <tt>conf-enabled/</tt> and <tt>sites-enabled/</tt> directories contain
            particular configuration snippets which manage modules, global configuration
            fragments, or virtual host configurations, respectively.
          </li>

          <li>
            They are activated by symlinking available
            configuration files from their respective
            *-available/ counterparts. These should be managed
            by using our helpers
            <tt>
                a2enmod,
                a2dismod,
            </tt>
            <tt>
                a2ensite,
                a2dissite,
             </tt>
                and
            <tt>
                a2enconf,
                a2disconf
            </tt>. See their respective man pages for detailed information.
          </li>

          <li>
            The binary is called apache2. Due to the use of
            environment variables, in the default configuration, apache2 needs to be
            started/stopped with <tt>/etc/init.d/apache2</tt> or <tt>apache2ctl</tt>.
            <b>Calling <tt>/usr/bin/apache2</tt> directly will not work</b> with the
            default configuration.
          </li>
  </ul>
</div>

<div class="section_header">
    <div id="docroot"></div>
        Document Roots
</div>

<div class="content_section_text">
    <p>
        By default, Debian does not allow access through the web browser to
        <em>any</em> file apart of those located in <tt>/var/www</tt>,
        <a href="http://httpd.apache.org/docs/2.4/mod/mod_userdir.html" rel="nofollow">public_html</a>
        directories (when enabled) and <tt>/usr/share</tt> (for web
        applications). If your site is using a web document root
        located elsewhere (such as in <tt>/srv</tt>) you may need to whitelist your
        document root directory in <tt>/etc/apache2/apache2.conf</tt>.
    </p>
    <p>
        The default Debian document root is <tt>/var/www/html</tt>. You
        can make your own virtual hosts under /var/www. This is different
        to previous releases which provides better security out of the box.
    </p>
</div>

<div class="section_header">
  <div id="bugs"></div>
        Reporting Problems
</div>
<div class="content_section_text">
```

```
        <p>
            Please use the <tt>reportbug</tt> tool to report bugs in the
            Apache2 package with Debian. However, check <a
            href="http://bugs.debian.org/cgi-bin/pkgreport.cgi?ordering=normal;archive=0;src=apache2;repeatmerged=0"
            rel="nofollow">existing bug reports</a> before reporting a new bug.
        </p>
        <p>
            Please report bugs specific to modules (such as PHP and others)
            to respective packages, not to the web server itself.
        </p>
      </div>



    </div>
   </div>
   <div class="validator">
   </div>
  </body>
</html>
```

4 Apache Hypertext Transfer Protocol (HTTP) Server NULL Pointer Dereference and Server Side Request Forgery (SSRF) Vulnerability — port 80/tcp

QID:	730313
Category:	CGI
Associated CVEs:	CVE-2021-44224
Vendor Reference:	Apache Security Advisory
Bugtraq ID:	-
Service Modified:	12/23/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
Apache HTTP Server is a free and open-source cross-platform web server software, released under the terms of Apache License 2.0.
A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery).
Affected Versions:
Apache HTTP Server 2.4.7 - 2.4.51
QID Detection Logic:(Unauthenticated)
This QID checks for vulnerable Apache Version by grabbing the banner from HTTP response

IMPACT:

Successful exploitation of the vulnerability may allow an attacker to redirect victim to a malicious server.

SOLUTION:
Customers are advised to update to Apache HTTP Server 2.4.52 or later. For more information, check Apache Security Advisory (https://httpd.apache.org/security/vulnerabilities_24.html)

Patch:
Following are links for downloading patches to fix the vulnerabilities:
Apache Security Advisory (https://httpd.apache.org/security/vulnerabilities_24.html)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Vulnerable Apache HTTP Server detected on port 80 -
Date: Mon, 01 Aug 2022 18:23:13 GMT
Server: Apache/2.4.51 (Debian)
Last-Modified: Mon, 20 Dec 2021 06:27:35 GMT
ETag: "29cd-5d38dfc099e6d"
Accept-Ranges: bytes
Content-Length: 10701
Vary: Accept-Encoding
Connection: close
Content-Type: text/html

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Apache2 Debian Default Page: It works</title>
    <style type="text/css" media="screen">
  * {
    margin: 0px 0px 0px 0px;
    padding: 0px 0px 0px 0px;
  }

  body, html {
    padding: 3px 3px 3px 3px;

    background-color: #D8DBE2;

    font-family: Verdana, sans-serif;
    font-size: 11pt;
    text-align: center;
  }

  div.main_page {
    position: relative;
    display: table;

    width: 800px;

    margin-bottom: 3px;
    margin-left: auto;
    margin-right: auto;
    paddinGET / HTTP/1.0
Host: kali
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:60.0) Gecko/20100101 Firefox/60.0
```

Vulnerable Version of Apache HTTP Server Detected on port: 80
HTTP/1.1 200 OK
Date: Mon, 01 Aug 2022 18:40:16 GMT
Server: Apache/2.4.51 (Debian)
Last-Modified: Mon, 20 Dec 2021 06:27:35 GMT
ETag: "29cd-5d38dfc099e6d"
Accept-Ranges: bytes
Content-Length: 10701
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Apache2 Debian Default Page: It works</title>
    <style type="text/css" media="screen">
  * {
    margin: 0px 0px 0px 0px;
    padding: 0px 0px 0px 0px;
  }

  body, html {
```

```
  padding: 3px 3px 3px 3px;

  background-color: #D8DBE2;

  font-family: Verdana, sans-serif;
  font-size: 11pt;
  text-align: center;
}

div.main_page {
  position: relative;
  display: table;

  width: 800px;

  margin-bottom: 3px;
  margin-left: auto;
  margin-right: auto;
  padding: 0px 0px 0px 0px;

  border-width: 2px;
  border-color: #212738;
  border-style: solid;

  background-color: #FFFFFF;

  text-align: center;
}

div.page_header {
  height: 99px;
  width: 100%;

  background-color: #F5F6F7;
}

div.page_header span {
  margin: 15px 0px 0px 50px;

  font-size: 180%;
  font-weight: bold;
}

div.page_header img {
  margin: 3px 0px 0px 40px;

  border: 0px 0px 0px;
}

div.table_of_contents {
  clear: left;

  min-width: 200px;

  margin: 3px 3px 3px 3px;

  background-color: #FFFFFF;

  text-align: left;
}

div.table_of_contents_item {
  clear: left;

  width: 100%;

  margin: 4px 0px 0px 0px;

  background-color: #FFFFFF;

  color: #000000;
  text-align: left;
}

div.table_of_contents_item a {
  margin: 6px 0px 0px 6px;
}
```

```
div.content_section {
  margin: 3px 3px 3px 3px;

  background-color: #FFFFFF;

  text-align: left;
}

div.content_section_text {
  padding: 4px 8px 4px 8px;

  color: #000000;
  font-size: 100%;
}

div.content_section_text pre {
  margin: 8px 0px 8px 0px;
  padding: 8px 8px 8px 8px;

  border-width: 1px;
  border-style: dotted;
  border-color: #000000;

  background-color: #F5F6F7;

  font-style: italic;
}

div.content_section_text p {
  margin-bottom: 6px;
}

div.content_section_text ul, div.content_section_text li {
  padding: 4px 8px 4px 16px;
}

div.section_header {
  padding: 3px 6px 3px 6px;

  background-color: #8E9CB2;

  color: #FFFFFF;
  font-weight: bold;
  font-size: 112%;
  text-align: center;
}

div.section_header_red {
  background-color: #CD214F;
}

div.section_header_grey {
  background-color: #9F9386;
}

.floating_element {
  position: relative;
  float: left;
}

div.table_of_contents_item a,
div.content_section_text a {
  text-decoration: none;
  font-weight: bold;
}

div.table_of_contents_item a:link,
div.table_of_contents_item a:visited,
div.table_of_contents_item a:active {
  color: #000000;
}

div.table_of_contents_item a:hover {
  background-color: #000000;

  color: #FFFFFF;
}
```

```
  div.content_section_text a:link,
  div.content_section_text a:visited,
   div.content_section_text a:active {
    background-color: #DCDFE6;

    color: #000000;
  }

  div.content_section_text a:hover {
    background-color: #000000;

    color: #DCDFE6;
  }

  div.validator {
  }
    </style>
  </head>
  <body>
    <div class="main_page">
      <div class="page_header floating_element">
        <img src="/icons/openlogo-75.png" alt="Debian Logo" class="floating_element"/>
        <span class="floating_element">
          Apache2 Debian Default Page
        </span>
      </div>
<!--       <div class="table_of_contents floating_element">
        <div class="section_header section_header_grey">
          TABLE OF CONTENTS
        </div>
        <div class="table_of_contents_item floating_element">
          <a href="#about">About</a>
        </div>
        <div class="table_of_contents_item floating_element">
          <a href="#changes">Changes</a>
        </div>
        <div class="table_of_contents_item floating_element">
          <a href="#scope">Scope</a>
        </div>
        <div class="table_of_contents_item floating_element">
          <a href="#files">Config files</a>
        </div>
      </div>
-->
      <div class="content_section floating_element">


        <div class="section_header section_header_red">
          <div id="about"></div>
          It works!
        </div>
        <div class="content_section_text">
          <p>
              This is the default welcome page used to test the correct
              operation of the Apache2 server after installation on Debian systems.
              If you can read this page, it means that the Apache HTTP server installed at
              this site is working properly. You should <b>replace this file</b> (located at
              <tt>/var/www/html/index.html</tt>) before continuing to operate your HTTP server.
          </p>


          <p>
              If you are a normal user of this web site and don't know what this page is
              about, this probably means that the site is currently unavailable due to
              maintenance.
              If the problem persists, please contact the site's administrator.
          </p>

        </div>
        <div class="section_header">
          <div id="changes"></div>
              Configuration Overview
        </div>
        <div class="content_section_text">
          <p>
              Debian's Apache2 default configuration is different from the
              upstream default configuration, and split into several files optimized for
              interaction with Debian tools. The configuration system is
```

fully documented in
/usr/share/doc/apache2/README.Debian.gz. Refer to this for the full
documentation. Documentation for the web server itself can be
found by accessing the manual if the <tt>apache2-doc</tt>
package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

<pre>
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled
| `-- *.conf
|-- sites-enabled
| `-- *.conf
</pre>

<tt>apache2.conf</tt> is the main configuration
file. It puts the pieces together by including all remaining configuration
files when starting up the web server.

<tt>ports.conf</tt> is always included from the
main configuration file. It is used to determine the listening ports for
incoming connections, and this file can be customized anytime.

Configuration files in the <tt>mods-enabled/</tt>,
<tt>conf-enabled/</tt> and <tt>sites-enabled/</tt> directories contain
particular configuration snippets which manage modules, global configuration
fragments, or virtual host configurations, respectively.

They are activated by symlinking available
configuration files from their respective
*-available/ counterparts. These should be managed
by using our helpers
<tt>
a2enmod,
a2dismod,
</tt>
<tt>
a2ensite,
a2dissite,
</tt>
and
<tt>
a2enconf,
a2disconf
</tt>. See their respective man pages for detailed information.

The binary is called apache2. Due to the use of
environment variables, in the default configuration, apache2 needs to be
started/stopped with <tt>/etc/init.d/apache2</tt> or <tt>apache2ctl</tt>.
Calling <tt>/usr/bin/apache2</tt> directly will not work with the
default configuration.

Document Roots

By default, Debian does not allow access through the web browser to
any file apart of those located in <tt>/var/www</tt>,
public_html
directories (when enabled) and <tt>/usr/share</tt> (for web
applications). If your site is using a web document root
located elsewhere (such as in <tt>/srv</tt>) you may need to whitelist your
document root directory in <tt>/etc/apache2/apache2.conf</tt>.

The default Debian document root is <tt>/var/www/html</tt>. You
can make your own virtual hosts under /var/www. This is different
to previous releases which provides better security out of the box.

Reporting Problems

Please use the <tt>reportbug</tt> tool to report bugs in the
Apache2 package with Debian. However, check <a
href="http://bugs.debian.org/cgi-bin/pkgreport.cgi?ordering=normal;archive=0;src=apache2;repeatmerged=0"
rel="nofollow">existing bug reports before reporting a new bug.

Please report bugs specific to modules (such as PHP and others)
to respective packages, not to the web server itself.

</body>
</html>

4 Apache Hypertext Transfer Protocol (HTTP) Server Out-of-bounds Write Vulnerability port 80/tcp

QID:	730403
Category:	CGI
Associated CVEs:	CVE-2022-23943, CVE-2022-22721, CVE-2022-22720, CVE-2022-22719
Vendor Reference:	Apache Security Advisory
Bugtraq ID:	-
Service Modified:	03/21/2022
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Apache HTTP Server is a free and open-source cross-platform web server software, released under the terms of Apache License 2.0.
CVE-2022-22719 - A carefully crafted request body can cause a read to a random memory area which could cause the process to crash.
CVE-2022-22720 - Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling
CVE-2022-22721 - If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes.
CVE-2022-23943 - Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data.
Affected Versions:
Apache HTTP Server 2.4 - 2.4.52

IMPACT:

Successful exploitation of the vulnerability may allow an attacker to redirect victim to a malicious server.

SOLUTION:
Customers are advised to update to Apache HTTP Server 2.4.53 or later. For more information, check Apache Security Advisory (https://httpd.apache.org/security/vulnerabilities_24.html)

Patch:
Following are links for downloading patches to fix the vulnerabilities:
Apache Security Advisory (https://httpd.apache.org/security/vulnerabilities_24.html)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Vulnerable Apache HTTP Server detected on port 80 -
Date: Mon, 01 Aug 2022 18:23:13 GMT
Server: Apache/2.4.51 (Debian)
Last-Modified: Mon, 20 Dec 2021 06:27:35 GMT
ETag: "29cd-5d38dfc099e6d"
Accept-Ranges: bytes
Content-Length: 10701
Vary: Accept-Encoding
Connection: close
Content-Type: text/html

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Apache2 Debian Default Page: It works</title>
    <style type="text/css" media="screen">
  * {
    margin: 0px 0px 0px 0px;
    padding: 0px 0px 0px 0px;
  }

  body, html {
    padding: 3px 3px 3px 3px;

    background-color: #D8DBE2;

    font-family: Verdana, sans-serif;
    font-size: 11pt;
    text-align: center;
  }

  div.main_page {
    position: relative;
    display: table;

    width: 800px;

    margin-bottom: 3px;
    margin-left: auto;
    margin-right: auto;
    paddinGET / HTTP/1.0
Host: kali
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:60.0) Gecko/20100101 Firefox/60.0
```

Vulnerable Version of Apache HTTP Server Detected on port: 80
HTTP/1.1 200 OK
Date: Mon, 01 Aug 2022 18:40:16 GMT
Server: Apache/2.4.51 (Debian)
Last-Modified: Mon, 20 Dec 2021 06:27:35 GMT
ETag: "29cd-5d38dfc099e6d"
Accept-Ranges: bytes

```
Content-Length: 10701
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Apache2 Debian Default Page: It works</title>
    <style type="text/css" media="screen">
  * {
    margin: 0px 0px 0px 0px;
    padding: 0px 0px 0px 0px;
  }

  body, html {
    padding: 3px 3px 3px 3px;

    background-color: #D8DBE2;

    font-family: Verdana, sans-serif;
    font-size: 11pt;
    text-align: center;
  }

  div.main_page {
    position: relative;
    display: table;

    width: 800px;

    margin-bottom: 3px;
    margin-left: auto;
    margin-right: auto;
    padding: 0px 0px 0px 0px;

    border-width: 2px;
    border-color: #212738;
    border-style: solid;

    background-color: #FFFFFF;

    text-align: center;
  }

  div.page_header {
    height: 99px;
    width: 100%;

    background-color: #F5F6F7;
  }

  div.page_header span {
    margin: 15px 0px 0px 50px;

    font-size: 180%;
    font-weight: bold;
  }

  div.page_header img {
    margin: 3px 0px 0px 40px;

    border: 0px 0px 0px;
  }

  div.table_of_contents {
    clear: left;

    min-width: 200px;

    margin: 3px 3px 3px 3px;

    background-color: #FFFFFF;

    text-align: left;
```

```
}

div.table_of_contents_item {
  clear: left;

  width: 100%;

  margin: 4px 0px 0px 0px;

  background-color: #FFFFFF;

  color: #000000;
  text-align: left;
}

div.table_of_contents_item a {
  margin: 6px 0px 0px 6px;
}

div.content_section {
  margin: 3px 3px 3px 3px;

  background-color: #FFFFFF;

  text-align: left;
}

div.content_section_text {
  padding: 4px 8px 4px 8px;

  color: #000000;
  font-size: 100%;
}

div.content_section_text pre {
  margin: 8px 0px 8px 0px;
  padding: 8px 8px 8px 8px;

  border-width: 1px;
  border-style: dotted;
  border-color: #000000;

  background-color: #F5F6F7;

  font-style: italic;
}

div.content_section_text p {
  margin-bottom: 6px;
}

div.content_section_text ul, div.content_section_text li {
  padding: 4px 8px 4px 16px;
}

div.section_header {
  padding: 3px 6px 3px 6px;

  background-color: #8E9CB2;

  color: #FFFFFF;
  font-weight: bold;
  font-size: 112%;
  text-align: center;
}

div.section_header_red {
  background-color: #CD214F;
}

div.section_header_grey {
  background-color: #9F9386;
}

.floating_element {
  position: relative;
  float: left;
}
```

```
  div.table_of_contents_item a,
  div.content_section_text a {
    text-decoration: none;
    font-weight: bold;
  }

  div.table_of_contents_item a:link,
  div.table_of_contents_item a:visited,
  div.table_of_contents_item a:active {
    color: #000000;
  }

  div.table_of_contents_item a:hover {
    background-color: #000000;

    color: #FFFFFF;
  }

  div.content_section_text a:link,
  div.content_section_text a:visited,
   div.content_section_text a:active {
    background-color: #DCDFE6;

    color: #000000;
  }

  div.content_section_text a:hover {
    background-color: #000000;

    color: #DCDFE6;
  }

  div.validator {
  }
    </style>
  </head>
  <body>
    <div class="main_page">
      <div class="page_header floating_element">
        <img src="/icons/openlogo-75.png" alt="Debian Logo" class="floating_element"/>
        <span class="floating_element">
          Apache2 Debian Default Page
        </span>
      </div>
<!--      <div class="table_of_contents floating_element">
        <div class="section_header section_header_grey">
          TABLE OF CONTENTS
        </div>
        <div class="table_of_contents_item floating_element">
          <a href="#about">About</a>
        </div>
        <div class="table_of_contents_item floating_element">
          <a href="#changes">Changes</a>
        </div>
        <div class="table_of_contents_item floating_element">
          <a href="#scope">Scope</a>
        </div>
        <div class="table_of_contents_item floating_element">
          <a href="#files">Config files</a>
        </div>
      </div>
-->
      <div class="content_section floating_element">


        <div class="section_header section_header_red">
          <div id="about"></div>
          It works!
        </div>
        <div class="content_section_text">
          <p>
              This is the default welcome page used to test the correct
              operation of the Apache2 server after installation on Debian systems.
              If you can read this page, it means that the Apache HTTP server installed at
              this site is working properly. You should <b>replace this file</b> (located at
              <tt>/var/www/html/index.html</tt>) before continuing to operate your HTTP server.
          </p>
```

If you are a normal user of this web site and don't know what this page is
about, this probably means that the site is currently unavailable due to
maintenance.
If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the
upstream default configuration, and split into several files optimized for
interaction with Debian tools. The configuration system is
fully documented in
/usr/share/doc/apache2/README.Debian.gz. Refer to this for the full
documentation. Documentation for the web server itself can be
found by accessing the manual if the <tt>apache2-doc</tt>
package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

<pre>
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled
| `-- *.conf
|-- sites-enabled
| `-- *.conf
</pre>

<tt>apache2.conf</tt> is the main configuration
file. It puts the pieces together by including all remaining configuration
files when starting up the web server.

<tt>ports.conf</tt> is always included from the
main configuration file. It is used to determine the listening ports for
incoming connections, and this file can be customized anytime.

Configuration files in the <tt>mods-enabled/</tt>,
<tt>conf-enabled/</tt> and <tt>sites-enabled/</tt> directories contain
particular configuration snippets which manage modules, global configuration
fragments, or virtual host configurations, respectively.

They are activated by symlinking available
configuration files from their respective
*-available/ counterparts. These should be managed
by using our helpers
<tt>
a2enmod,
a2dismod,
</tt>
<tt>
a2ensite,
a2dissite,
</tt>
and
<tt>
a2enconf,
a2disconf

```
                </tt>. See their respective man pages for detailed information.
              </li>

              <li>
                The binary is called apache2. Due to the use of
                environment variables, in the default configuration, apache2 needs to be
                started/stopped with <tt>/etc/init.d/apache2</tt> or <tt>apache2ctl</tt>.
                <b>Calling <tt>/usr/bin/apache2</tt> directly will not work</b> with the
                default configuration.
              </li>
        </ul>
      </div>

      <div class="section_header">
        <div id="docroot"></div>
          Document Roots
      </div>

      <div class="content_section_text">
        <p>
          By default, Debian does not allow access through the web browser to
          <em>any</em> file apart of those located in <tt>/var/www</tt>,
          <a href="http://httpd.apache.org/docs/2.4/mod/mod_userdir.html" rel="nofollow">public_html</a>
          directories (when enabled) and <tt>/usr/share</tt> (for web
          applications). If your site is using a web document root
          located elsewhere (such as in <tt>/srv</tt>) you may need to whitelist your
          document root directory in <tt>/etc/apache2/apache2.conf</tt>.
        </p>
        <p>
          The default Debian document root is <tt>/var/www/html</tt>. You
          can make your own virtual hosts under /var/www. This is different
          to previous releases which provides better security out of the box.
        </p>
      </div>

      <div class="section_header">
        <div id="bugs"></div>
          Reporting Problems
      </div>
      <div class="content_section_text">
        <p>
          Please use the <tt>reportbug</tt> tool to report bugs in the
          Apache2 package with Debian. However, check <a
          href="http://bugs.debian.org/cgi-bin/pkgreport.cgi?ordering=normal;archive=0;src=apache2;repeatmerged=0"
          rel="nofollow">existing bug reports</a> before reporting a new bug.
        </p>
        <p>
          Please report bugs specific to modules (such as PHP and others)
          to respective packages, not to the web server itself.
        </p>
      </div>




    </div>
  </div>
  <div class="validator">
  </div>
 </body>
</html>
```

Information Gathered (29)

3 Content-Security-Policy HTTP Security Header Not Detected port 80/tcp

QID:	48001
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	Content-Security-Policy
Bugtraq ID:	-
Service Modified:	03/11/2019
User Modified:	-
Edited:	No

PCI Vuln: No

THREAT:
The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).
QID Detection Logic:
This QID detects the absence of the Content-Security-Policy HTTP header by transmitting a GET request.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Content-Security-Policy HTTP Header missing on port 80.
GET / HTTP/1.0
Host: kali

 3 Content-Security-Policy HTTP Security Header Not Detected port 8000/tcp

QID:	48001
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	Content-Security-Policy
Bugtraq ID:	-
Service Modified:	03/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).
QID Detection Logic:
This QID detects the absence of the Content-Security-Policy HTTP header by transmitting a GET request.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Content-Security-Policy HTTP Header missing on port 8000.
GET / HTTP/1.0
Host: kali:8000

2 Operating System Detected

QID:	45017
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/04/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.
1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.
Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.
2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).
3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.
4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:

Not applicable.

SOLUTION:

Not applicable.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Operating System	Technique	ID
Ubuntu/Linux	TCP/IP Fingerprint	U7254:80

2 Host Uptime Based on TCP TimeStamp Option

QID:	82063
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	05/29/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.
Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Based on TCP timestamps obtained via port 80, the host's uptime is 16 days, 17 hours, and 25 minutes.
The TCP timestamps from the host are in units of 1 milliseconds.

2 Web Server HTTP Protocol Versions — port 80/tcp

QID:	45266
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:
Remote Web Server supports HTTP version 1.x on 80 port.GET / HTTP/1.1

2 Web Server HTTP Protocol Versions port 8000/tcp

QID:	45266
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Remote Web Server supports HTTP version 1.x on 8000 port.GET / HTTP/1.1

1 DNS Host Name

QID:	6
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
192.168.50.142	kali

1 Host Scan Time - Scanner

QID:	45038
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/16/2022
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Scan duration: 1757 seconds

Start time: Mon, Aug 01 2022, 18:22:05 GMT

End time: Mon, Aug 01 2022, 18:51:22 GMT

1 Host Names Found

QID:	45039
Category:	Information gathering
Associated CVEs:	-

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/27/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
kali	FQDN

1 Apache HTTP Server Detected

QID:	45391
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/03/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating systems including UNIX and Windows. The goal of this project is to provide a secure, efficient and extensible server that provides HTTP services in sync with the current HTTP standards.
Apache HTTP Server was detected on the target.
QID Detection Logic (Authenticated):
Operating System: Linux
The detection looks for Apache HTTP Server installation path using ps command. The version is extracted from the Apache HTTP Server's binary.
Operating System: Windows
This QID checks Windows registry to see if Apache HTTP Server is installed. If found, it displays the installed version.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Apache web server detected on port 80 -
Date: Mon, 01 Aug 2022 18:23:13 GMT
Server: Apache/2.4.51 (Debian)
Last-Modified: Mon, 20 Dec 2021 06:27:35 GMT
ETag: "29cd-5d38dfc099e6d"
Accept-Ranges: bytes
Content-Length: 10701
Vary: Accept-Encoding
Connection: close
Content-Type: text/html

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Apache2 Debian Default Page: It works</title>
    <style type="text/css" media="screen">
  * {
    margin: 0px 0px 0px 0px;
    padding: 0px 0px 0px 0px;
  }

  body, html {
    padding: 3px 3px 3px 3px;

    background-color: #D8DBE2;

    font-family: Verdana, sans-serif;
    font-size: 11pt;
    text-align: center;
  }

  div.main_page {
    position: relative;
    display: table;

    width: 800px;

    margin-bottom: 3px;
    margin-left: auto;
    margin-right: auto;
    paddin
```

1 Scan Activity per Port

QID:	45426
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or

services on which requests time out.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	80	1:49:31
TCP	8000	1:46:52

1 Open TCP Services List

QID:	82023
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/15/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
80	www-http	World Wide Web HTTP	http	
8000	irdmi	iRDMI	http	

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Time Stamp (type=14 code=0)	Time Stamp Request	18:22:49 GMT
Unreachable (type=3 code=3)	UDP Port 1	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 30336	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 80	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 121	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 6051	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 518	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 123	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 41154	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 500	Port Unreachable
Unreachable (type=3 code=2)	IP with High Protocol	Protocol Unreachable
Unreachable (type=3 code=3)	UDP Port 3391	Port Unreachable

1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/19/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Average change between subsequent TCP initial sequence numbers is 921330700 with a standard deviation of 766292328. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5673 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/27/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.
Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP ID changes observed (network order) for port 80: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Duration: 5 milli seconds

1 Default Web Page port 80/tcp

QID:	12230
Category:	CGI
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/16/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: kali



HTTP/1.1 200 OK
Date: Mon, 01 Aug 2022 18:28:28 GMT
Server: Apache/2.4.51 (Debian)
Last-Modified: Mon, 20 Dec 2021 06:27:35 GMT
ETag: "29cd-5d38dfc099e6d"
Accept-Ranges: bytes
Content-Length: 10701
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Apache2 Debian Default Page: It works</title>
    <style type="text/css" media="screen">
  * {
    margin: 0px 0px 0px 0px;
    padding: 0px 0px 0px 0px;
  }

  body, html {
    padding: 3px 3px 3px 3px;

    background-color: #D8DBE2;
```

```
  font-family: Verdana, sans-serif;
  font-size: 11pt;
  text-align: center;
}

div.main_page {
  position: relative;
  display: table;

  width: 800px;

  margin-bottom: 3px;
  margin-left: auto;
  margin-right: auto;
  padding: 0px 0px 0px 0px;

  border-width: 2px;
  border-color: #212738;
  border-style: solid;

  background-color: #FFFFFF;

  text-align: center;
}

div.page_header {
  height: 99px;
  width: 100%;

  background-color: #F5F6F7;
}

div.page_header span {
  margin: 15px 0px 0px 50px;

  font-size: 180%;
  font-weight: bold;
}

div.page_header img {
  margin: 3px 0px 0px 40px;

  border: 0px 0px 0px;
}

div.table_of_contents {
  clear: left;

  min-width: 200px;

  margin: 3px 3px 3px 3px;

  background-color: #FFFFFF;

  text-align: left;
}

div.table_of_contents_item {
  clear: left;

  width: 100%;

  margin: 4px 0px 0px 0px;

  background-color: #FFFFFF;

  color: #000000;
  text-align: left;
}

div.table_of_contents_item a {
  margin: 6px 0px 0px 6px;
}

div.content_section {
  margin: 3px 3px 3px 3px;
```

```
  background-color: #FFFFFF;

  text-align: left;
}

div.content_section_text {
  padding: 4px 8px 4px 8px;

  color: #000000;
  font-size: 100%;
}

div.content_section_text pre {
  margin: 8px 0px 8px 0px;
  padding: 8px 8px 8px 8px;

  border-width: 1px;
  border-style: dotted;
  border-color: #000000;

  background-color: #F5F6F7;

  font-style: italic;
}

div.content_section_text p {
  margin-bottom: 6px;
}

div.content_section_text ul, div.content_section_text li {
  padding: 4px 8px 4px 16px;
}

div.section_header {
  padding: 3px 6px 3px 6px;

  background-color: #8E9CB2;

  color: #FFFFFF;
  font-weight: bold;
  font-size: 112%;
  text-align: center;
}

div.section_header_red {
  background-color: #CD214F;
}

div.section_header_grey {
  background-color: #9F9386;
}

.floating_element {
  position: relative;
  float: left;
}

div.table_of_contents_item a,
div.content_section_text a {
  text-decoration: none;
  font-weight: bold;
}

div.table_of_contents_item a:link,
div.table_of_contents_item a:visited,
div.table_of_contents_item a:active {
  color: #000000;
}

div.table_of_contents_item a:hover {
  background-color: #000000;

  color: #FFFFFF;
}

div.content_section_text a:link,
div.content_section_text a:visited,
 div.content_section_text a:active {
```

```
    background-color: #DCDFE6;

    color: #000000;
  }

  div.content_section_text a:hover {
    background-color: #000000;

    color: #DCDFE6;
  }

  div.validator {
  }
    </style>
  </head>
  <body>
    <div class="main_page">
      <div class="page_header floating_element">
        <img src="/icons/openlogo-75.png" alt="Debian Logo" class="floating_element"/>
        <span class="floating_element">
          Apache2 Debian Default Page
        </span>
      </div>
<!--       <div class="table_of_contents floating_element">
        <div class="section_header section_header_grey">
          TABLE OF CONTENTS
        </div>
        <div class="table_of_contents_item floating_element">
          <a href="#about">About</a>
        </div>
        <div class="table_of_contents_item floating_element">
          <a href="#changes">Changes</a>
        </div>
        <div class="table_of_contents_item floating_element">
          <a href="#scope">Scope</a>
        </div>
        <div class="table_of_contents_item floating_element">
          <a href="#files">Config files</a>
        </div>
      </div>
-->
      <div class="content_section floating_element">


        <div class="section_header section_header_red">
          <div id="about"></div>
          It works!
        </div>
        <div class="content_section_text">
          <p>
              This is the default welcome page used to test the correct
              operation of the Apache2 server after installation on Debian systems.
              If you can read this page, it means that the Apache HTTP server installed at
              this site is working properly. You should <b>replace this file</b> (located at
              <tt>/var/www/html/index.html</tt>) before continuing to operate your HTTP server.
          </p>


          <p>
              If you are a normal user of this web site and don't know what this page is
              about, this probably means that the site is currently unavailable due to
              maintenance.
              If the problem persists, please contact the site's administrator.
          </p>

        </div>
        <div class="section_header">
          <div id="changes"></div>
              Configuration Overview
        </div>
        <div class="content_section_text">
          <p>
              Debian's Apache2 default configuration is different from the
              upstream default configuration, and split into several files optimized for
              interaction with Debian tools. The configuration system is
              <b>fully documented in
              /usr/share/doc/apache2/README.Debian.gz</b>. Refer to this for the full
              documentation. Documentation for the web server itself can be
```

found by accessing the manual if the <tt>apache2-doc</tt>
package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

<pre>
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled
| `-- *.conf
|-- sites-enabled
| `-- *.conf
</pre>

<tt>apache2.conf</tt> is the main configuration
file. It puts the pieces together by including all remaining configuration
files when starting up the web server.

<tt>ports.conf</tt> is always included from the
main configuration file. It is used to determine the listening ports for
incoming connections, and this file can be customized anytime.

Configuration files in the <tt>mods-enabled/</tt>,
<tt>conf-enabled/</tt> and <tt>sites-enabled/</tt> directories contain
particular configuration snippets which manage modules, global configuration
fragments, or virtual host configurations, respectively.

They are activated by symlinking available
configuration files from their respective
*-available/ counterparts. These should be managed
by using our helpers
<tt>
a2enmod,
a2dismod,
</tt>
<tt>
a2ensite,
a2dissite,
</tt>
and
<tt>
a2enconf,
a2disconf
</tt>. See their respective man pages for detailed information.

The binary is called apache2. Due to the use of
environment variables, in the default configuration, apache2 needs to be
started/stopped with <tt>/etc/init.d/apache2</tt> or <tt>apache2ctl</tt>.
Calling <tt>/usr/bin/apache2</tt> directly will not work with the
default configuration.

Document Roots

By default, Debian does not allow access through the web browser to
any file apart of those located in <tt>/var/www</tt>,

public_html
directories (when enabled) and <tt>/usr/share</tt> (for web
applications). If your site is using a web document root
located elsewhere (such as in <tt>/srv</tt>) you may need to whitelist your
document root directory in <tt>/etc/apache2/apache2.conf</tt>.

The default Debian document root is <tt>/var/www/html</tt>. You
can make your own virtual hosts under /var/www. This is different
to previous releases which provides better security out of the box.

Reporting Problems

Please use the <tt>reportbug</tt> tool to report bugs in the
Apache2 package with Debian. However, check <a
href="http://bugs.debian.org/cgi-bin/pkgreport.cgi?ordering=normal;archive=0;src=apache2;repeatmerged=0"
rel="nofollow">existing bug reports before reporting a new bug.

Please report bugs specific to modules (such as PHP and others)
to respective packages, not to the web server itself.

</body>
</html>

1 Default Web Page (Follow HTTP Redirection) port 80/tcp

QID:	13910
Category:	CGI
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: kali



HTTP/1.1 200 OK
Date: Mon, 01 Aug 2022 18:35:57 GMT
Server: Apache/2.4.51 (Debian)
Last-Modified: Mon, 20 Dec 2021 06:27:35 GMT
ETag: "29cd-5d38dfc099e6d"
Accept-Ranges: bytes
Content-Length: 10701
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Apache2 Debian Default Page: It works</title>
    <style type="text/css" media="screen">
  * {
    margin: 0px 0px 0px 0px;
    padding: 0px 0px 0px 0px;
  }

  body, html {
    padding: 3px 3px 3px 3px;

    background-color: #D8DBE2;

    font-family: Verdana, sans-serif;
    font-size: 11pt;
    text-align: center;
  }

  div.main_page {
    position: relative;
    display: table;

    width: 800px;

    margin-bottom: 3px;
    margin-left: auto;
    margin-right: auto;
    padding: 0px 0px 0px 0px;

    border-width: 2px;
    border-color: #212738;
    border-style: solid;

    background-color: #FFFFFF;

    text-align: center;
  }

  div.page_header {
    height: 99px;
    width: 100%;

    background-color: #F5F6F7;
  }

  div.page_header span {
    margin: 15px 0px 0px 50px;

    font-size: 180%;
    font-weight: bold;
  }

  div.page_header img {
```

```
  margin: 3px 0px 0px 40px;

  border: 0px 0px 0px;
}

div.table_of_contents {
  clear: left;

  min-width: 200px;

  margin: 3px 3px 3px 3px;

  background-color: #FFFFFF;

  text-align: left;
}

div.table_of_contents_item {
  clear: left;

  width: 100%;

  margin: 4px 0px 0px 0px;

  background-color: #FFFFFF;

  color: #000000;
  text-align: left;
}

div.table_of_contents_item a {
  margin: 6px 0px 0px 6px;
}

div.content_section {
  margin: 3px 3px 3px 3px;

  background-color: #FFFFFF;

  text-align: left;
}

div.content_section_text {
  padding: 4px 8px 4px 8px;

  color: #000000;
  font-size: 100%;
}

div.content_section_text pre {
  margin: 8px 0px 8px 0px;
  padding: 8px 8px 8px 8px;

  border-width: 1px;
  border-style: dotted;
  border-color: #000000;

  background-color: #F5F6F7;

  font-style: italic;
}

div.content_section_text p {
  margin-bottom: 6px;
}

div.content_section_text ul, div.content_section_text li {
  padding: 4px 8px 4px 16px;
}

div.section_header {
  padding: 3px 6px 3px 6px;

  background-color: #8E9CB2;

  color: #FFFFFF;
  font-weight: bold;
  font-size: 112%;
```

```
    text-align: center;
  }

  div.section_header_red {
    background-color: #CD214F;
  }

  div.section_header_grey {
    background-color: #9F9386;
  }

  .floating_element {
    position: relative;
    float: left;
  }

  div.table_of_contents_item a,
  div.content_section_text a {
    text-decoration: none;
    font-weight: bold;
  }

  div.table_of_contents_item a:link,
  div.table_of_contents_item a:visited,
  div.table_of_contents_item a:active {
    color: #000000;
  }

  div.table_of_contents_item a:hover {
    background-color: #000000;

    color: #FFFFFF;
  }

  div.content_section_text a:link,
  div.content_section_text a:visited,
   div.content_section_text a:active {
    background-color: #DCDFE6;

    color: #000000;
  }

  div.content_section_text a:hover {
    background-color: #000000;

    color: #DCDFE6;
  }

  div.validator {
  }
    </style>
  </head>
  <body>
    <div class="main_page">
      <div class="page_header floating_element">
        <img src="/icons/openlogo-75.png" alt="Debian Logo" class="floating_element"/>
        <span class="floating_element">
          Apache2 Debian Default Page
        </span>
      </div>
<!--      <div class="table_of_contents floating_element">
        <div class="section_header section_header_grey">
          TABLE OF CONTENTS
        </div>
        <div class="table_of_contents_item floating_element">
          <a href="#about">About</a>
        </div>
        <div class="table_of_contents_item floating_element">
          <a href="#changes">Changes</a>
        </div>
        <div class="table_of_contents_item floating_element">
          <a href="#scope">Scope</a>
        </div>
        <div class="table_of_contents_item floating_element">
          <a href="#files">Config files</a>
        </div>
      </div>
-->
```

```
    <div class="content_section floating_element">


      <div class="section_header section_header_red">
        <div id="about"></div>
        It works!
      </div>
      <div class="content_section_text">
        <p>
            This is the default welcome page used to test the correct
            operation of the Apache2 server after installation on Debian systems.
            If you can read this page, it means that the Apache HTTP server installed at
            this site is working properly. You should <b>replace this file</b> (located at
            <tt>/var/www/html/index.html</tt>) before continuing to operate your HTTP server.
        </p>


        <p>
            If you are a normal user of this web site and don't know what this page is
            about, this probably means that the site is currently unavailable due to
            maintenance.
            If the problem persists, please contact the site's administrator.
        </p>

      </div>
      <div class="section_header">
        <div id="changes"></div>
            Configuration Overview
      </div>
      <div class="content_section_text">
        <p>
            Debian's Apache2 default configuration is different from the
            upstream default configuration, and split into several files optimized for
            interaction with Debian tools. The configuration system is
            <b>fully documented in
            /usr/share/doc/apache2/README.Debian.gz</b>. Refer to this for the full
            documentation. Documentation for the web server itself can be
            found by accessing the <a href="/manual">manual</a> if the <tt>apache2-doc</tt>
            package was installed on this server.

        </p>
        <p>
            The configuration layout for an Apache2 web server installation on Debian systems is as follows:
        </p>
        <pre>
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
        </pre>
        <ul>
                <li>
                  <tt>apache2.conf</tt> is the main configuration
                  file. It puts the pieces together by including all remaining configuration
                  files when starting up the web server.
                </li>

                <li>
                  <tt>ports.conf</tt> is always included from the
                  main configuration file. It is used to determine the listening ports for
                  incoming connections, and this file can be customized anytime.
                </li>

                <li>
                  Configuration files in the <tt>mods-enabled/</tt>,
                  <tt>conf-enabled/</tt> and <tt>sites-enabled/</tt> directories contain
                  particular configuration snippets which manage modules, global configuration
                  fragments, or virtual host configurations, respectively.
                </li>

                <li>
                  They are activated by symlinking available
```

```
                configuration files from their respective
                *-available/ counterparts. These should be managed
                by using our helpers
                <tt>
                    a2enmod,
                    a2dismod,
                </tt>
                <tt>
                    a2ensite,
                    a2dissite,
                 </tt>
                    and
                <tt>
                    a2enconf,
                    a2disconf
                </tt>. See their respective man pages for detailed information.
              </li>

              <li>
                The binary is called apache2. Due to the use of
                environment variables, in the default configuration, apache2 needs to be
                started/stopped with <tt>/etc/init.d/apache2</tt> or <tt>apache2ctl</tt>.
                <b>Calling <tt>/usr/bin/apache2</tt> directly will not work</b> with the
                default configuration.
              </li>
    </ul>
  </div>

  <div class="section_header">
     <div id="docroot"></div>
        Document Roots
  </div>

  <div class="content_section_text">
     <p>
        By default, Debian does not allow access through the web browser to
        <em>any</em> file apart of those located in <tt>/var/www</tt>,
        <a href="http://httpd.apache.org/docs/2.4/mod/mod_userdir.html" rel="nofollow">public_html</a>
        directories (when enabled) and <tt>/usr/share</tt> (for web
        applications). If your site is using a web document root
        located elsewhere (such as in <tt>/srv</tt>) you may need to whitelist your
        document root directory in <tt>/etc/apache2/apache2.conf</tt>.
     </p>
     <p>
        The default Debian document root is <tt>/var/www/html</tt>. You
        can make your own virtual hosts under /var/www. This is different
        to previous releases which provides better security out of the box.
     </p>
  </div>

  <div class="section_header">
    <div id="bugs"></div>
        Reporting Problems
  </div>
  <div class="content_section_text">
    <p>
        Please use the <tt>reportbug</tt> tool to report bugs in the
        Apache2 package with Debian. However, check <a
        href="http://bugs.debian.org/cgi-bin/pkgreport.cgi?ordering=normal;archive=0;src=apache2;repeatmerged=0"
        rel="nofollow">existing bug reports</a> before reporting a new bug.
    </p>
    <p>
        Please report bugs specific to modules (such as PHP and others)
        to respective packages, not to the web server itself.
    </p>
  </div>




    </div>
  </div>
  <div class="validator">
  </div>
 </body>
</html>
```

1 HTTP Methods Returned by OPTIONS Request port 80/tcp

QID:	45056
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Allow: OPTIONS,HEAD,GET,POST

1 Apache Default Installation/Welcome Page Detected port 80/tcp

QID:	48065
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Apache default installation or "Welcome" page is installed on this server. This usually indicates a newly installed server which has not yet been configured properly and which may not be known about.
Detection Logic(unauthenticated):
QID will check for the apache default Installation/Welcome Page on apache server.

IMPACT:
Apache is installed by default and the user may not be aware that the web server is running. These servers are rarely patched and rarely monitored, providing hackers with a convenient target that is not likely to trip any alarms.

SOLUTION:
Customers are recommended to disable default Apache welcome configuration.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
HTTP/1.1 200 OK
Date: Mon, 01 Aug 2022 18:28:28 GMT
Server: Apache/2.4.51 (Debian)
Last-Modified: Mon, 20 Dec 2021 06:27:35 GMT
ETag: "29cd-5d38dfc099e6d"
Accept-Ranges: bytes
Content-Length: 10701
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Apache2 Debian Default Page: It works</title>
    <style type="text/css" media="screen">
  * {
    margin: 0px 0px 0px 0px;
    padding: 0px 0px 0px 0px;
  }

  body, html {
    padding: 3px 3px 3px 3px;

    background-color: #D8DBE2;

    font-family: Verdana, sans-serif;
    font-size: 11pt;
    text-align: center;
  }

  div.main_page {
    position: relative;
    display: table;

    width: 800px;

    margin-bottom: 3px;
    margin-left: auto;
    margin-right: auto;
    padding: 0px 0px 0px 0px;

    border-width: 2px;
    border-color: #212738;
    border-style: solid;

    background-color: #FFFFFF;

    text-align: center;
  }

  div.page_header {
    height: 99px;
    width: 100%;

    background-color: #F5F6F7;
  }

  div.page_header span {
    margin: 15px 0px 0px 50px;

    font-size: 180%;
    font-weight: bold;
```

```
}

div.page_header img {
  margin: 3px 0px 0px 40px;

  border: 0px 0px 0px;
}

div.table_of_contents {
  clear: left;

  min-width: 200px;

  margin: 3px 3px 3px 3px;

  background-color: #FFFFFF;

  text-align: left;
}

div.table_of_contents_item {
  clear: left;

  width: 100%;

  margin: 4px 0px 0px 0px;

  background-color: #FFFFFF;

  color: #000000;
  text-align: left;
}

div.table_of_contents_item a {
  margin: 6px 0px 0px 6px;
}

div.content_section {
  margin: 3px 3px 3px 3px;

  background-color: #FFFFFF;

  text-align: left;
}

div.content_section_text {
  padding: 4px 8px 4px 8px;

  color: #000000;
  font-size: 100%;
}

div.content_section_text pre {
  margin: 8px 0px 8px 0px;
  padding: 8px 8px 8px 8px;

  border-width: 1px;
  border-style: dotted;
  border-color: #000000;

  background-color: #F5F6F7;

  font-style: italic;
}

div.content_section_text p {
  margin-bottom: 6px;
}

div.content_section_text ul, div.content_section_text li {
  padding: 4px 8px 4px 16px;
}

div.section_header {
  padding: 3px 6px 3px 6px;

  background-color: #8E9CB2;
```

```
    color: #FFFFFF;
    font-weight: bold;
    font-size: 112%;
    text-align: center;
  }

  div.section_header_red {
    background-color: #CD214F;
  }

  div.section_header_grey {
    background-color: #9F9386;
  }

  .floating_element {
    position: relative;
    float: left;
  }

  div.table_of_contents_item a,
  div.content_section_text a {
    text-decoration: none;
    font-weight: bold;
  }

  div.table_of_contents_item a:link,
  div.table_of_contents_item a:visited,
  div.table_of_contents_item a:active {
    color: #000000;
  }

  div.table_of_contents_item a:hover {
    background-color: #000000;

    color: #FFFFFF;
  }

  div.content_section_text a:link,
  div.content_section_text a:visited,
   div.content_section_text a:active {
    background-color: #DCDFE6;

    color: #000000;
  }

  div.content_section_text a:hover {
    background-color: #000000;

    color: #DCDFE6;
  }

  div.validator {
  }
    </style>
  </head>
  <body>
    <div class="main_page">
      <div class="page_header floating_element">
        <img src="/icons/openlogo-75.png" alt="Debian Logo" class="floating_element"/>
        <span class="floating_element">
          Apache2 Debian Default Page
        </span>
      </div>
<!--      <div class="table_of_contents floating_element">
        <div class="section_header section_header_grey">
          TABLE OF CONTENTS
        </div>
        <div class="table_of_contents_item floating_element">
          <a href="#about">About</a>
        </div>
        <div class="table_of_contents_item floating_element">
          <a href="#changes">Changes</a>
        </div>
        <div class="table_of_contents_item floating_element">
          <a href="#scope">Scope</a>
        </div>
        <div class="table_of_contents_item floating_element">
          <a href="#files">Config files</a>
```

```
      </div>
    </div>
-->
    <div class="content_section floating_element">


      <div class="section_header section_header_red">
        <div id="about"></div>
        It works!
      </div>
      <div class="content_section_text">
        <p>
            This is the default welcome page used to test the correct
            operation of the Apache2 server after installation on Debian systems.
            If you can read this page, it means that the Apache HTTP server installed at
            this site is working properly. You should <b>replace this file</b> (located at
            <tt>/var/www/html/index.html</tt>) before continuing to operate your HTTP server.
        </p>


        <p>
            If you are a normal user of this web site and don't know what this page is
            about, this probably means that the site is currently unavailable due to
            maintenance.
            If the problem persists, please contact the site's administrator.
        </p>

      </div>
      <div class="section_header">
        <div id="changes"></div>
            Configuration Overview
      </div>
      <div class="content_section_text">
        <p>
            Debian's Apache2 default configuration is different from the
            upstream default configuration, and split into several files optimized for
            interaction with Debian tools. The configuration system is
            <b>fully documented in
            /usr/share/doc/apache2/README.Debian.gz</b>. Refer to this for the full
            documentation. Documentation for the web server itself can be
            found by accessing the <a href="/manual">manual</a> if the <tt>apache2-doc</tt>
            package was installed on this server.

        </p>
        <p>
            The configuration layout for an Apache2 web server installation on Debian systems is as follows:
        </p>
        <pre>
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
        </pre>
        <ul>
                <li>
                  <tt>apache2.conf</tt> is the main configuration
                  file. It puts the pieces together by including all remaining configuration
                  files when starting up the web server.
                </li>

                <li>
                  <tt>ports.conf</tt> is always included from the
                  main configuration file. It is used to determine the listening ports for
                  incoming connections, and this file can be customized anytime.
                </li>

                <li>
                  Configuration files in the <tt>mods-enabled/</tt>,
                  <tt>conf-enabled/</tt> and <tt>sites-enabled/</tt> directories contain
                  particular configuration snippets which manage modules, global configuration
                  fragments, or virtual host configurations, respectively.
                </li>
```

```
                <li>
                  They are activated by symlinking available
                  configuration files from their respective
                  *-available/ counterparts. These should be managed
                  by using our helpers
                  <tt>
                      a2enmod,
                      a2dismod,
                  </tt>
                  <tt>
                      a2ensite,
                      a2dissite,
                   </tt>
                      and
                  <tt>
                      a2enconf,
                      a2disconf
                  </tt>. See their respective man pages for detailed information.
                </li>

                <li>
                  The binary is called apache2. Due to the use of
                  environment variables, in the default configuration, apache2 needs to be
                  started/stopped with <tt>/etc/init.d/apache2</tt> or <tt>apache2ctl</tt>.
                  <b>Calling <tt>/usr/bin/apache2</tt> directly will not work</b> with the
                  default configuration.
                </li>
    </ul>
  </div>

  <div class="section_header">
     <div id="docroot"></div>
        Document Roots
  </div>

  <div class="content_section_text">
     <p>
        By default, Debian does not allow access through the web browser to
        <em>any</em> file apart of those located in <tt>/var/www</tt>,
        <a href="http://httpd.apache.org/docs/2.4/mod/mod_userdir.html" rel="nofollow">public_html</a>
        directories (when enabled) and <tt>/usr/share</tt> (for web
        applications). If your site is using a web document root
        located elsewhere (such as in <tt>/srv</tt>) you may need to whitelist your
        document root directory in <tt>/etc/apache2/apache2.conf</tt>.
     </p>
     <p>
        The default Debian document root is <tt>/var/www/html</tt>. You
        can make your own virtual hosts under /var/www. This is different
        to previous releases which provides better security out of the box.
     </p>
  </div>

  <div class="section_header">
    <div id="bugs"></div>
        Reporting Problems
  </div>
  <div class="content_section_text">
    <p>
        Please use the <tt>reportbug</tt> tool to report bugs in the
        Apache2 package with Debian. However, check <a
        href="http://bugs.debian.org/cgi-bin/pkgreport.cgi?ordering=normal;archive=0;src=apache2;repeatmerged=0"
        rel="nofollow">existing bug reports</a> before reporting a new bug.
    </p>
    <p>
        Please report bugs specific to modules (such as PHP and others)
        to respective packages, not to the web server itself.
    </p>
  </div>



    </div>
  </div>
  <div class="validator">
  </div>
</body>
```

</html>

Apache Default Installation/Welcome Page Detected on port 80.

1 HTTP Response Method and Header Information Collected port 80/tcp

QID:	48118
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
HTTP header and method information collected on port 80.

GET / HTTP/1.0
Host: kali

HTTP/1.1 200 OK
Date: Mon, 01 Aug 2022 18:28:28 GMT
Server: Apache/2.4.51 (Debian)
Last-Modified: Mon, 20 Dec 2021 06:27:35 GMT
ETag: "29cd-5d38dfc099e6d"
Accept-Ranges: bytes
Content-Length: 10701
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

1 Referrer-Policy HTTP Security Header Not Detected port 80/tcp

QID:	48131
Category:	Information gathering
Associated CVEs:	-

Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:
1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin
QID Detection Logic(Unauthenticated):
If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.
References:
- https://www.w3.org/TR/referrer-policy/ (https://www.w3.org/TR/referrer-policy/)
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 80 port.

 1 Web Server Version port 80/tcp

QID:	86000
Category:	Web server
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/20/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

A web server is server software, or hardware dedicated to running this software, that can satisfy client requests on the World Wide Web.

IMPACT:

N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Apache/2.4.51 (Debian)

1 Web Server Supports HTTP Request Pipelining port 80/tcp

QID:	86565
Category:	Web server
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/22/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.
The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:
Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Spliting style attacks.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
GET / HTTP/1.1
Host:192.168.50.142:80

GET /Q_Evasive/ HTTP/1.1
Host:192.168.50.142:80

1 List of Web Directories port 80/tcp

QID:	86672

Category:	Web server
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/javascript/	brute force
/icons/	brute force
/icons/	web page

1 Default Web Page port 8000/tcp

QID:	12230
Category:	CGI
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/16/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.0
Host: kali:8000

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>Directory listing for /</title>
</head>
<body>
<h1>Directory listing for /</h1>
<hr>

<hr>
</body>
</html>

1 Default Web Page (Follow HTTP Redirection) port 8000/tcp

QID:	13910
Category:	CGI
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

GET / HTTP/1.0
Host: kali:8000

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>Directory listing for /</title>
</head>
<body>

<h1>Directory listing for /</h1>
<hr>

<hr>
</body>
</html>

1 HTTP Response Method and Header Information Collected port 8000/tcp

QID:	48118
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
HTTP header and method information collected on port 8000.

GET / HTTP/1.0
Host: kali:8000

HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/3.9.8
Date: Mon, 01 Aug 2022 18:23:35 GMT
Content-type: text/html; charset=utf-8
Content-Length: 297

1 Referrer-Policy HTTP Security Header Not Detected port 8000/tcp

QID:	48131
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	Referrer-Policy

Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:
1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin
QID Detection Logic(Unauthenticated):
If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.
References:
- https://www.w3.org/TR/referrer-policy/ (https://www.w3.org/TR/referrer-policy/)
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 8000 port.

1 Directory Listing Enabled On Web Service — port 8000/tcp

QID:	48180
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/28/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Directory listing allows users to view all the files (including source files) under a directory served by the website.
QID Detection Logic:(Unauthenticated)
This QID sends GET request to verify if directory listing is enabled or not.

IMPACT:

N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Directory Listing enabled on port: 8000
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>Directory listing for /</title>
</head>
<body>
<h1>Directory listing for /</h1>
<hr>

<hr>
</body>
</html>

Appendix

Hosts Scanned (IP)

192.168.50.42, 192.168.50.142

Target distribution across scanner appliances

teste : 192.168.50.42, 192.168.50.142

Options Profile

Initial Options

Scan Settings

Ports:	
Scanned TCP Ports:	Standard Scan
Scanned UDP Ports:	Standard Scan
Scan Dead Hosts:	Off
Close Vulnerabilities on Dead Hosts Count:	Off
Purge old host data when OS changes:	Off
Load Balancer Detection:	Off
Perform 3-way Handshake:	Off
Vulnerability Detection:	Complete
Intrusive Checks:	Excluded
Password Brute Forcing:	
System:	Disabled
Custom:	Disabled
Authentication:	
Windows:	Disabled
Unix/Cisco/Network SSH:	Disabled
Oracle:	Disabled
Oracle Listener:	Disabled
SNMP:	Disabled
VMware:	Disabled
DB2:	Disabled
HTTP:	Disabled
MySQL:	Disabled
Tomcat Server:	Disabled
MongoDB:	Disabled
Palo Alto Networks Firewall:	Disabled
Jboss Server:	Disabled
Oracle WebLogic Server:	Disabled
MariaDB:	Disabled
InformixDB:	Disabled
MS Exchange Server:	Disabled
Oracle HTTP Server:	Disabled
MS SharePoint:	Disabled
Kubernetes:	Disabled
SAP IQ:	Disabled
SAP HANA:	Disabled
Azure MS SQL:	Disabled
Neo4j:	Disabled

Nginx:	Disabled
Overall Performance:	Normal
Authenticated Scan Certificate Discovery:	Disabled
Test Authentication:	Disabled
Hosts to Scan in Parallel:	
Use Appliance Parallel ML Scaling:	Off
External Scanners:	15
Scanner Appliances:	30
Processes to Run in Parallel:	
Total Processes:	10
HTTP Processes:	10
Packet (Burst) Delay:	Medium
Port Scanning and Host Discovery:	
Intensity:	Normal
Dissolvable Agent:	
Dissolvable Agent (for this profile):	Disabled
Windows Share Enumeration:	Disabled
Windows Directory Search:	Disabled
Lite OS Discovery:	Disabled
Host Alive Testing:	Disabled
Do Not Overwrite OS:	Disabled

System Authentication

System Authentication Records:

Include system created authentication records in scans: Disabled

Advanced Settings

Host Discovery:	TCP Standard Scan, UDP Standard Scan, ICMP On
Ignore firewall-generated TCP RST packets:	Off
Ignore all TCP RST packets:	Off
Ignore firewall-generated TCP SYN-ACK packets:	Off
Do not send TCP ACK or SYN-ACK packets during host discovery:	Off

Report Legend

Vulnerability Levels

A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.

Severity	Level	Description
1	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
4	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.

Severity	Level	Description
5	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Potential Vulnerability Levels

A potential vulnerability is one which we cannot confirm exists. The only way to verify the existence of such vulnerabilities on your network would be to perform an intrusive scan, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate these potential vulnerabilities further.

Severity	Level	Description
1	Minimal	If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
2	Medium	If this vulnerability exists on your system, intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
3	Serious	If this vulnerability exists on your system, intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
4	Critical	If this vulnerability exists on your system, intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
5	Urgent	If this vulnerability exists on your system, intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Information Gathered

Information Gathered includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

Severity	Level	Description
1	Minimal	Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls.
2	Medium	Intruders may be able to determine the operating system running on the host, and view banner versions.
3	Serious	Intruders may be able to detect highly sensitive data, such as global system user lists.