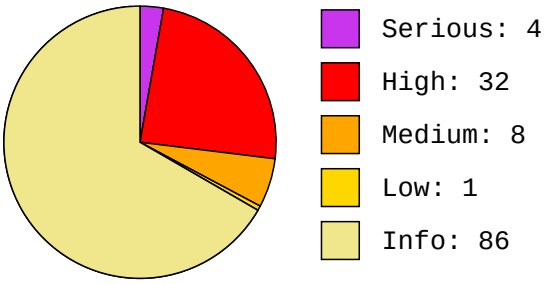
AlienVault: I.T Security Vulnerability Report

Job Name:	9.13.2021-control_scan	Scan time:	2020-01-24 22:35:36
Profile:	Default - Non destructive Full and Fast scan	Generated:	2020-01-24 22:36:41

Total number of vulnerabilities identified on 3 system(s)



Total number of vulnerabilities identified per system

HostIP	HostName	Serious	High	Med	Low	Info
172.20.1.129	Host-172-20-1-129	--	--	--	--	15
172.20.1.131	Host-172-20-1-131	4	32	8	1	61
172.20.1.132	Host-172-20-1-132	--	--	--	--	10

172.20.1.129	Host-172-20-1-129

Info:

SSH Protocol Algorithms Supported
Risk: Info
Application: ssh
Port: 22
Protocol: tcp
ScriptID: 105565
Vulnerability Detection Result:
The following options are supported by the remote ssh service:
kex_algorithms:
curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,diffie-hellman-group14-sha1
server_host_key_algorithms:
ssh-rsa,rsa-sha2-512,rsa-sha2-256,ecdsa-sha2-nistp256,ssh-ed25519
encryption_algorithms_client_to_server:
chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com
encryption_algorithms_server_to_client:
chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com
mac_algorithms_client_to_server:
umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1
mac_algorithms_server_to_client:
umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1
compression_algorithms_client_to_server:
none,zlib@openssh.com
compression_algorithms_server_to_client:
none,zlib@openssh.com
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
This script detects which algorithms and languages are supported by the remote SSH Service
CVSS Base Score: 0.0
Family name: Service detection
Category: infos

Summary: NOSUMMARY
Version: $Revision: 13581 $

Info:

SSH Protocol Versions Supported
Risk: Info
Application: ssh
Port: 22
Protocol: tcp
ScriptID: 100259
Vulnerability Detection Result:
The remote SSH Server supports the following SSH Protocol Versions:
2.0
SSHv2 Fingerprint(s):
ecdsa-sha2-nistp256: da:76:1e:16:7f:a6:8a:eb:9b:5e:93:28:28:80:aa:de
ssh-rsa: 49:4c:39:29:36:a0:45:68:b4:77:fa:52:e1:cd:b1:fe
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
Identification of SSH protocol versions supported by the remote
SSH Server. Also reads the corresponding fingerprints from the service.
The following versions are tried: 1.33, 1.5, 1.99 and 2.0
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: This script is Copyright (C) 2009 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 13594 $

Info:

SSH Server type and version
Risk: Info
Application: ssh
Port: 22
Protocol: tcp
ScriptID: 10267
Vulnerability Detection Result:
Remote SSH server banner: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
Remote SSH supported authentication: password,publickey
Remote SSH text/login banner: (not available)
This is probably:
- OpenSSH
Concluded from remote connection attempt with credentials:
Login: OpenVAS-VT
Password: OpenVAS-VT
Summary:
This detects the SSH Server's type and version by connecting to the server
and processing the buffer received.
This information gives potential attackers additional information about the system they are attacking.
Versions and Types should be omitted where possible.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Product detection
Category: infos
Copyright: This script is Copyright (C) 1999 SecuriTeam
Summary: NOSUMMARY
Version: 2019-06-05T03:32:14+0000

Info:

Traceroute
Risk: Info
Application: general
Port: 0
Protocol: tcp
ScriptID: 51662
Vulnerability Detection Result:
Here is the route from 172.20.1.127 to 172.20.1.129:
172.20.1.127
?
Summary:
A traceroute from the scanning server to the target system was
conducted. This traceroute is provided primarily for informational value only. In the vast
majority of cases, it does not represent a vulnerability. However, if the displayed traceroute
contains any private addresses that should not have been publicly visible, then you have an
issue you need to correct.
Solution:
Block unwanted packets from escaping your network.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: General
Category: infos

Summary: NOSUMMARY
Version: $Revision: 10411 $

Info:

Apache Web Server Version Detection
Risk: Info
Application: http
Port: 80
Protocol: tcp
ScriptID: 900498
Vulnerability Detection Result:
Detected Apache
Version: 2.4.29
Location: 80/tcp
CPE: cpe:/a:apache:http_server:2.4.29
Concluded from version/product identification result:
Server: Apache/2.4.29
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
Detects the installed version of Apache Web Server
The script detects the version of Apache HTTP Server on remote host and sets the KB.
CVSS Base Score: 0.0
Family name: Product detection
Category: infos
Copyright: Copyright (C) 2009 SecPod
Summary: NOSUMMARY
Version: $Revision: 10290 $

Info:

CGI Scanning Consolidation
Risk: Info
Application: http
Port: 80
Protocol: tcp
ScriptID: 111038
Vulnerability Detection Result:
The Hostname/IP "172.20.1.129" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable generic web application scanning" option within the "Global variable settings" of the scan config in use.
Requests to this service are done via HTTP/1.1.
This service seems to be able to host PHP scripts.
This service seems to be NOT able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 9.0.3)" was used to access the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI scanning. You can enable this again with the "Add historic /scripts and /cgi-bin to directories for CGI scanning" option within the "Global variable settings" of the scan config in use.
The following directories were used for CGI scanning:
http://172.20.1.129/
While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards
The following directories were excluded from CGI scanning because the "Regex pattern to exclude directories from CGI scanning" setting of the NVT "Global variable settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was: "/(index\.php|image|img|css|js$|js/|javascript|style|theme|icon|jquery|graphic|grafik|picture|bilder|thumbnail|media/|skins?/)"
http://172.20.1.129/icons
Summary:
The script consolidates various information for CGI scanning.
This information is based on the following scripts / settings:
- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use
- The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use
If you think any of this information is wrong please report it to the referenced community portal.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
References:
https://community.greenbone.net/c/vulnerability-tests
CVSS Base Score: 0.0
Family name: Web application abuses
Category: infos
Copyright: This script is Copyright (C) 2015 SCHUTZWERK GmbH
Summary: NOSUMMARY
Version: $Revision: 13679 $

Info:

CPE Inventory
Risk: Info
Application: general
Port: 0
Protocol: CPE-T
ScriptID: 810002
Vulnerability Detection Result:
172.20.1.129|cpe:/a:apache:http_server:2.4.29
172.20.1.129|cpe:/a:openbsd:openssh:7.6p1
172.20.1.129|cpe:/o:canonical:ubuntu_linux:18.04
Summary:
This routine uses information collected by other routines about
CPE identities of operating systems, services and
applications detected during the scan.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
References:
http://cpe.mitre.org/
CVSS Base Score: 0.0
Family name: Service detection
Category: end
Copyright: Copyright (c) 2009 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 14324 $

Info:

HTTP Security Headers Detection
Risk: Info
Application: http
Port: 80
Protocol: tcp
ScriptID: 112081
Vulnerability Detection Result:
Missing Headers

Content-Security-Policy
Referrer-Policy
X-Content-Type-Options
X-Frame-Options
X-Permitted-Cross-Domain-Policies
X-XSS-Protection
Summary:
All known security headers are being checked on the host. On completion a report will hand back whether a specific security header
has been implemented (including its value) or is missing on the target.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
References:
https://www.owasp.org/index.php/OWASP_Secure_Headers_Project
https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#tab=Headers
https://securityheaders.io/
CVSS Base Score: 0.0
Family name: General
Category: infos

Summary: NOSUMMARY
Version: $Revision: 10899 $

Info:

HTTP Server type and version
Risk: Info
Application: http
Port: 80
Protocol: tcp
ScriptID: 10107
Vulnerability Detection Result:
The remote web server type is :
Apache/2.4.29 (Ubuntu)
Solution : You can set the directive "ServerTokens Prod" to limit
the information emanating from the server in its response headers.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Solution:
- Configure your server to use an alternate name like
'Wintendo httpD w/Dotmatrix display'
- Be sure to remove common logos like apache_pb.gif.
- With Apache, you can set the directive 'ServerTokens Prod' to limit
the information emanating from the server in its response headers.
Summary:
This detects the HTTP Server's type and version.
CVSS Base Score: 0.0
Family name: Web Servers
Category: infos

Summary: NOSUMMARY
Version: $Revision: 11585 $

Info:

Nikto (NASL wrapper)
Risk: Info
Application: http
Port: 80
Protocol: tcp
ScriptID: 14260
Vulnerability Detection Result:
Here is the Nikto report:
Unknown option: useragent
-config+ Use this config file
-Display+ Turn on/off display outputs
-dbcheck check database and other key files for syntax errors
-Format+ save file (-o) format
-Help Extended help information
-host+ target host
-id+ Host authentication to use, format is id:pass or id:pass:realm
-list-plugins List all available plugins
-output+ Write output to this file
-nossl Disables using SSL
-no404 Disables 404 checks
-Plugins+ List of plugins to run (default: ALL)
-port+ Port to use (default 80)
-root+ Prepend root value to all requests, format is /directory
-ssl Force ssl mode on port
-Tuning+ Scan tuning
-timeout+ Timeout for requests (default 10 seconds)
-update Update databases and plugins from CIRT.net
-Version Print plugin and database versions
-vhost+ Virtual host (for Host header)
+ requires a value
Note: This is the short help output. Use -H for full help text.
Summary:
This plugin uses nikto to find weak CGI scripts and other known issues
regarding web server security. See the preferences section for configuration options.
Note: The plugin needs the 'nikto' or 'nikto.pl' binary found within the PATH of the user running the scanner and needs to be executable for this user. The existence of this binary is checked and reported separately within 'Availability of scanner helper tools' (OID: 1.3.6.1.4.1.25623.1.0.810000).
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Web application abuses
Category: infos
Copyright: This script is Copyright (C) 2004 Michel Arboi
Summary: NOSUMMARY
Version: $Revision: 13985 $

Info:

OpenSSH Detection Consolidation
Risk: Info
Application: general
Port: 0
Protocol: tcp
ScriptID: 108577
Vulnerability Detection Result:
Detected OpenSSH Server
Version: 7.6p1
Location: 22/tcp
CPE: cpe:/a:openbsd:openssh:7.6p1
Concluded from version/product identification result:
SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
Summary:
The script reports a detected OpenSSH including the
version number.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
References:
https://www.openssh.com/
CVSS Base Score: 0.0
Family name: Product detection
Category: unknown

Version: 2019-05-23T06:42:35+0000

Info:

OS Detection Consolidation and Reporting
Risk: Info
Application: general
Port: 0
Protocol: tcp
ScriptID: 105937
Vulnerability Detection Result:
Best matching OS:
OS: Ubuntu
Version: 18.04
CPE: cpe:/o:canonical:ubuntu_linux:18.04
Found by NVT: 1.3.6.1.4.1.25623.1.0.105586 (SSH OS Identification)
Concluded from SSH banner on port 22/tcp: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
Setting key "Host/runs_unixoide" based on this information
Other OS detections (in order of reliability):
OS: Ubuntu
Version: 18.04
CPE: cpe:/o:canonical:ubuntu_linux:18.04
Found by NVT: 1.3.6.1.4.1.25623.1.0.111067 (HTTP OS Identification)
Concluded from HTTP Server banner on port 80/tcp: Server: Apache/2.4.29 (Ubuntu)
OS: Ubuntu
CPE: cpe:/o:canonical:ubuntu_linux
Found by NVT: 1.3.6.1.4.1.25623.1.0.111067 (HTTP OS Identification)
Concluded from HTTP Server default page on port 80/tcp: <title>Apache2 Ubuntu Default Page
Summary:
This script consolidates the OS information detected by several NVTs and tries to find the best matching OS.
Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional information
which might help to improve the OS detection.
If any of this information is wrong or could be improved please consider to report these to the referenced community portal.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
References:
https://community.greenbone.net/c/vulnerability-tests
CVSS Base Score: 0.0
Family name: Product detection
Category: infos
Copyright: This script is Copyright (C) 2016 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: 2019-06-01T08:20:43+0000

Info:

Ping Host
Risk: Info
Application: general
Port: 0
Protocol: tcp
ScriptID: 100315
Vulnerability Detection Result:
The alive test was not launched because no method was selected.
Summary:
This check tries to determine whether a remote host is up (alive).
Several methods are used for this depending on configuration of this check. Whether a host is up can be detected in 3 different ways:
- A ICMP message is sent to the host and a response is taken as alive sign.
- An ARP request is sent and a response is taken as alive sign.
- A number of typical TCP services (namely the 20 top ports of nmap) are tried and their presence is taken as alive sign.
None of the methods is failsafe. It depends on network and/or host configurations whether they succeed or not. Both, false positives and false negatives can occur.
Therefore the methods are configurable.
If you select to not mark unreachable hosts as dead, no alive detections are executed and the host is assumed to be available for scanning.
In case it is configured that hosts are never marked as dead, this can cause considerable timeouts and therefore a long scan duration in case the hosts are in fact not available.
The available methods might fail for the following reasons:
- ICMP: This might be disabled for a environment and would then cause false negatives as hosts are believed to be dead that actually are alive. In contrast it is also possible that a Firewall between the scanner and the target host is answering to the ICMP message and thus hosts are believed to be alive that actually are dead.
- TCP ping: Similar to the ICMP case a Firewall between the scanner and the target might answer to the sent probes and thus hosts are believed to be alive that actually are dead.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Port scanners
Category: scanner

Summary: NOSUMMARY
Version: 2019-05-24T11:20:30+0000

Info:

Services
Risk: Info
Application: ssh
Port: 22
Protocol: tcp
ScriptID: 10330
Vulnerability Detection Result:
An ssh server is running on this port
Summary:
This routine attempts to guess which service is running on the
remote ports. For instance, it searches for a web server which could listen on another port than
80 or 443 and makes this information available for other check routines.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>
Summary: NOSUMMARY
Version: $Revision: 13541 $

Info:

Services
Risk: Info
Application: http
Port: 80
Protocol: tcp
ScriptID: 10330
Vulnerability Detection Result:
A web server is running on this port
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
This routine attempts to guess which service is running on the
remote ports. For instance, it searches for a web server which could listen on another port than
80 or 443 and makes this information available for other check routines.
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>
Summary: NOSUMMARY
Version: $Revision: 13541 $

172.20.1.131	Host-172-20-1-131

Serious:

Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)
Risk: Serious
Application: microsoft-ds
Port: 445
Protocol: tcp
ScriptID: 810676
Solution:
The vendor has released updates. Please see the references for more information.
Summary:
This host is missing a critical security
update according to Microsoft Bulletin MS17-010.
Affected Software/OS:
Microsoft Windows 10 x32/x64 Edition
Microsoft Windows Server 2012 Edition
Microsoft Windows Server 2016
Microsoft Windows 8.1 x32/x64 Edition
Microsoft Windows Server 2012 R2 Edition
Microsoft Windows 7 x32/x64 Edition Service Pack 1
Microsoft Windows Vista x32/x64 Edition Service Pack 2
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2
Vulnerability Detection Method:
Send the crafted SMB transaction request
with fid = 0 and check the response to confirm the vulnerability.
Impact:
Successful exploitation will allow remote
attackers to gain the ability to execute code on the target server, also
could lead to information disclosure from the server.
Insight:
Multiple flaws exist due to the way that the
Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.
CVSS Base Vector:
AV:N/AC:M/Au:N/C:C/I:C/A:C
References:
https://support.microsoft.com/en-in/kb/4013078
https://technet.microsoft.com/library/security/MS17-010
https://github.com/rapid7/metasploit-framework/pull/8167/files
CVSS Base Score: 9.3
Family name: Windows : Microsoft Bulletins
Category: attack

Summary: NOSUMMARY
Version: 2019-05-03T10:54:50+0000

Serious:

OpenSSL End of Life Detection (Windows)
Risk: Serious
Application: https
Port: 443
Protocol: tcp
ScriptID: 113027
Vulnerability Detection Result:
The "OpenSSL" version on the remote host has reached the end of life.
CPE: cpe:/a:openssl:openssl:1.0.2p
Installed version: 1.0.2p
Location/URL: 443/tcp
EOL version: 1.0.2
EOL date: 2019-12-31
CVSS Base Vector:
AV:N/AC:L/Au:N/C:C/I:C/A:C
Vulnerability Detection Method:
Checks if a vulnerable version is present on the target host.
Impact:
An end of life version of OpenSSL is not receiving any security updates from the vendor. Unfixed security vulnerabilities
might be leveraged by an attacker to compromise the security of this host.
Solution:
Update the OpenSSL version on the remote host to a still supported version.
Summary:
The OpenSSL version on the remote host has reached the end of
life and should not be used anymore.
References:
https://www.openssl.org/policies/releasestrat.html
CVSS Base Score: 10.0
Family name: Web application abuses
Category: infos
Copyright: Copyright (C) 2017 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 13898 $

Serious:

PHP End Of Life Detection (Windows)
Risk: Serious
Application: https
Port: 443
Protocol: tcp
ScriptID: 105888
Vulnerability Detection Result:
The "PHP" version on the remote host has reached the end of life.
CPE: cpe:/a:php:php:7.0.33
Installed version: 7.0.33
EOL version: 7.0
EOL date: 2018-12-03
Solution:
Update the PHP version on the remote host to a still supported version.
Summary:
The PHP version on the remote host has reached the end of life and should
not be used anymore.
Vulnerability Detection Method:
Checks if a vulnerable version is present on the target host.
Impact:
An end of life version of PHP is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.
Insight:
Each release branch of PHP is fully supported for two years from its initial stable release.
During this period, bugs and security issues that have been reported are fixed and are released in regular point releases.
After this two year period of active support, each branch is then supported for an additional year for critical security issues only. Releases during this period are made on an as-needed basis: there may be multiple point releases, or none,
depending on the number of reports.
Once the three years of support are completed, the branch reaches its end of life and is no longer supported.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:C/I:C/A:C
References:
https://secure.php.net/supported-versions.php
https://secure.php.net/eol.php
CVSS Base Score: 10.0
Family name: Web application abuses
Category: infos
Copyright: Copyright (C) 2016 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 12363 $

Serious:

PHP End Of Life Detection (Windows)
Risk: Serious
Application: http
Port: 80
Protocol: tcp
ScriptID: 105888
Vulnerability Detection Result:
The "PHP" version on the remote host has reached the end of life.
CPE: cpe:/a:php:php:7.0.33
Installed version: 7.0.33
EOL version: 7.0
EOL date: 2018-12-03
Summary:
The PHP version on the remote host has reached the end of life and should
not be used anymore.
Solution:
Update the PHP version on the remote host to a still supported version.
Vulnerability Detection Method:
Checks if a vulnerable version is present on the target host.
Impact:
An end of life version of PHP is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.
Insight:
Each release branch of PHP is fully supported for two years from its initial stable release.
During this period, bugs and security issues that have been reported are fixed and are released in regular point releases.
After this two year period of active support, each branch is then supported for an additional year for critical security issues only. Releases during this period are made on an as-needed basis: there may be multiple point releases, or none,
depending on the number of reports.
Once the three years of support are completed, the branch reaches its end of life and is no longer supported.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:C/I:C/A:C
References:
https://secure.php.net/supported-versions.php
https://secure.php.net/eol.php
CVSS Base Score: 10.0
Family name: Web application abuses
Category: infos
Copyright: Copyright (C) 2016 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 12363 $

High:

Apache HTTP Server 2.4.37 mod_ssl DoS Vulnerability (Windows)
Risk: High
Application: https
Port: 443
Protocol: tcp
ScriptID: 141961
Vulnerability Detection Result:
Installed version: 2.4.37
Fixed version: 2.4.38
Solution:
Update to version 2.4.38 or later.
Summary:
A bug exists in the way mod_ssl handled client renegotiations. A remote
attacker could send a carefully crafted request that would cause mod_ssl to enter a loop leading to a denial of service. This bug can be only triggered with Apache HTTP Server version 2.4.37 when using OpenSSL version 1.1.1 or
later, due to an interaction in changes to handling of renegotiation attempts.
Affected Software/OS:
Apache HTTP server version 2.4.37.
Vulnerability Detection Method:
Checks if a vulnerable version is present on the target host.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:P
References:
https://httpd.apache.org/security/vulnerabilities_24.html
CVSS Base Score: 5.0
Family name: Web Servers
Category: unknown

Version: $Revision: 13547 $

High:

Apache HTTP Server 2.4.37 mod_ssl DoS Vulnerability (Windows)
Risk: High
Application: http
Port: 80
Protocol: tcp
ScriptID: 141961
Vulnerability Detection Result:
Installed version: 2.4.37
Fixed version: 2.4.38
Affected Software/OS:
Apache HTTP server version 2.4.37.
Vulnerability Detection Method:
Checks if a vulnerable version is present on the target host.
Solution:
Update to version 2.4.38 or later.
Summary:
A bug exists in the way mod_ssl handled client renegotiations. A remote
attacker could send a carefully crafted request that would cause mod_ssl to enter a loop leading to a denial of service. This bug can be only triggered with Apache HTTP Server version 2.4.37 when using OpenSSL version 1.1.1 or
later, due to an interaction in changes to handling of renegotiation attempts.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:P
References:
https://httpd.apache.org/security/vulnerabilities_24.html
CVSS Base Score: 5.0
Family name: Web Servers
Category: unknown

Version: $Revision: 13547 $

High:

SSL/TLS: Certificate Expired
Risk: High
Application: https
Port: 443
Protocol: tcp
ScriptID: 103955
Vulnerability Detection Result:
The certificate of the remote service expired on 2019-11-08 23:48:47.
Certificate details:
subject ...: CN=localhost
subject alternative names (SAN):
None
issued by .: CN=localhost
serial ....: 00B5C752C98781B503
valid from : 2009-11-10 23:48:47 UTC
valid until: 2019-11-08 23:48:47 UTC
fingerprint (SHA-1): B0238C547A905BFA119C4E8BACCAEACF36491FF6
fingerprint (SHA-256): 016973380C0F1DF00BD9593ED8D5EFA3706CD6DF7993F6141272B80522ACDD23
Solution:
Replace the SSL/TLS certificate by a new one.
Summary:
The remote server's SSL/TLS certificate has already expired.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:P/A:N
Insight:
This script checks expiry dates of certificates associated with
SSL/TLS-enabled services on the target and reports whether any have already expired.
CVSS Base Score: 5.0
Family name: SSL and TLS
Category: infos
Copyright: This script is Copyright (C) 2013 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 11103 $

High:

Apache HTTP Server < 2.4.39 mod_ssl Access Control Bypass Vulnerability (Windows)
Risk: High
Application: general
Port: 0
Protocol: tcp
ScriptID: 142223
Vulnerability Detection Result:
Installed version: 2.4.37
Fixed version: 2.4.39
CVSS Base Vector:
AV:N/AC:M/Au:S/C:P/I:P/A:P
Summary:
In Apache HTTP Server a bug in mod_ssl when using per-location client
certificate verification with TLSv1.3 allowed a client supporting Post-Handshake Authentication to bypass
configured access control restrictions.
Solution:
Update to version 2.4.39 or later.
Affected Software/OS:
Apache HTTP server version 2.4.37 and 2.4.38.
Vulnerability Detection Method:
Checks if a vulnerable version is present on the target host.
References:
https://httpd.apache.org/security/vulnerabilities_24.html
CVSS Base Score: 6.0
Family name: Web Servers
Category: unknown

Version: 2019-04-15T07:08:44+0000

High:

Untrusted SSL/TLS Certificate Authorities
Risk: High
Application: https
Port: 443
Protocol: tcp
ScriptID: 113054
Vulnerability Detection Result:
The certificate of the remote service is signed by the following untrusted Certificate Authority:
Issuer: CN=localhost
Certificate details:
subject ...: CN=localhost
subject alternative names (SAN):
None
issued by .: CN=localhost
serial ....: 00B5C752C98781B503
valid from : 2009-11-10 23:48:47 UTC
valid until: 2019-11-08 23:48:47 UTC
fingerprint (SHA-1): B0238C547A905BFA119C4E8BACCAEACF36491FF6
fingerprint (SHA-256): 016973380C0F1DF00BD9593ED8D5EFA3706CD6DF7993F6141272B80522ACDD23
Solution:
Replace the SSL/TLS certificate with one signed by a trusted certificate authority.
Summary:
The service is using a SSL/TLS certificate from a known untrusted certificate authority.
An attacker could use this for MitM attacks, accessing sensible data and other attacks.
Vulnerability Detection Method:
The script reads the certificate used by the target host and checks if it was
signed by an untrusted certificate authority.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:P/A:N
CVSS Base Score: 5.0
Family name: SSL and TLS
Category: infos
Copyright: Copyright (C) 2017 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 11874 $

High:

Apache HTTP Server < 2.4.39 mod_ssl Access Control Bypass Vulnerability (Windows)
Risk: High
Application: general
Port: 0
Protocol: tcp
ScriptID: 142223
Vulnerability Detection Result:
Installed version: 2.4.37
Fixed version: 2.4.39
CVSS Base Vector:
AV:N/AC:M/Au:S/C:P/I:P/A:P
Vulnerability Detection Method:
Checks if a vulnerable version is present on the target host.
Affected Software/OS:
Apache HTTP server version 2.4.37 and 2.4.38.
Solution:
Update to version 2.4.39 or later.
Summary:
In Apache HTTP Server a bug in mod_ssl when using per-location client
certificate verification with TLSv1.3 allowed a client supporting Post-Handshake Authentication to bypass
configured access control restrictions.
References:
https://httpd.apache.org/security/vulnerabilities_24.html
CVSS Base Score: 6.0
Family name: Web Servers
Category: unknown

Version: 2019-04-15T07:08:44+0000

High:

Apache HTTP Server < 2.4.39 URL Normalization Vulnerability (Windows)
Risk: High
Application: general
Port: 0
Protocol: tcp
ScriptID: 142229
Vulnerability Detection Result:
Installed version: 2.4.37
Fixed version: 2.4.39
CVSS Base Vector:
AV:N/AC:L/Au:N/C:P/I:N/A:N
Affected Software/OS:
Apache HTTP server version 2.4.38 and prior.
Vulnerability Detection Method:
Checks if a vulnerable version is present on the target host.
Solution:
Update to version 2.4.39 or later.
Summary:
When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.
References:
https://httpd.apache.org/security/vulnerabilities_24.html
CVSS Base Score: 5.0
Family name: Web Servers
Category: unknown

Version: 2019-06-17T06:50:08+0000

High:

Apache HTTP Server < 2.4.39 URL Normalization Vulnerability (Windows)
Risk: High
Application: general
Port: 0
Protocol: tcp
ScriptID: 142229
Vulnerability Detection Result:
Installed version: 2.4.37
Fixed version: 2.4.39
Summary:
When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.
Solution:
Update to version 2.4.39 or later.
Affected Software/OS:
Apache HTTP server version 2.4.38 and prior.
Vulnerability Detection Method:
Checks if a vulnerable version is present on the target host.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:P/I:N/A:N
References:
https://httpd.apache.org/security/vulnerabilities_24.html
CVSS Base Score: 5.0
Family name: Web Servers
Category: unknown

Version: 2019-06-17T06:50:08+0000

High:

Apache HTTP Server < 2.4.38 HTTP/2 DoS Vulnerability (Windows)
Risk: High
Application: general
Port: 0
Protocol: tcp
ScriptID: 141965
Vulnerability Detection Result:
Installed version: 2.4.37
Fixed version: 2.4.38
Affected Software/OS:
Apache HTTP server version 2.4.37 and prior.
Vulnerability Detection Method:
Checks if a vulnerable version is present on the target host.
Solution:
Update to version 2.4.38 or later.
Summary:
By sending request bodies in a slow loris way to plain resources, the h2
stream for that request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 connections. A possible mitigation is to not enable the h2 protocol.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:P
References:
https://httpd.apache.org/security/vulnerabilities_24.html
CVSS Base Score: 5.0
Family name: Web Servers
Category: unknown

Version: $Revision: 13547 $

High:

Check if Mailserver answer to VRFY and EXPN requests
Risk: High
Application: smtp
Port: 25
Protocol: tcp
ScriptID: 100072
Vulnerability Detection Result:
'VRFY root' produces the following answer: 550 Address not valid for this site.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:P
Insight:
VRFY and EXPN ask the server for information about an address. They are
inherently unusable through firewalls, gateways, mail exchangers for part-time hosts, etc.
Summary:
The Mailserver on this host answers to VRFY and/or EXPN requests.
Solution:
Disable VRFY and/or EXPN on your Mailserver.
For postfix add 'disable_vrfy_command=yes' in 'main.cf'.
For Sendmail add the option 'O PrivacyOptions=goaway'.
It is suggested that, if you really want to publish this type of information, you use a mechanism
that legitimate users actually know about, such as Finger or HTTP.
References:
http://cr.yp.to/smtp/vrfy.html
CVSS Base Score: 5.0
Family name: SMTP problems
Category: infos
Copyright: This script is Copyright (C) 2009 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 13470 $

High:

DCE/RPC and MSRPC Services Enumeration Reporting
Risk: High
Application: msrpc
Port: 135
Protocol: tcp
ScriptID: 10736
Vulnerability Detection Result:
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP protocol:
Port: 49152/tcp
UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
Endpoint: ncacn_ip_tcp:172.20.1.131[49152]
Port: 49153/tcp
UUID: 06bba54a-be05-49f9-b0a0-30f790261023, version 1
Endpoint: ncacn_ip_tcp:172.20.1.131[49153]
Annotation: Security Center
UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1
Endpoint: ncacn_ip_tcp:172.20.1.131[49153]
Annotation: NRP server endpoint
UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
Endpoint: ncacn_ip_tcp:172.20.1.131[49153]
Annotation: DHCP Client LRPC Endpoint
UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1
Endpoint: ncacn_ip_tcp:172.20.1.131[49153]
Annotation: DHCPv6 Client LRPC Endpoint
UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
Endpoint: ncacn_ip_tcp:172.20.1.131[49153]
Annotation: Event log TCPIP
Port: 49154/tcp
UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1
Endpoint: ncacn_ip_tcp:172.20.1.131[49154]
Annotation: AppInfo
UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
Endpoint: ncacn_ip_tcp:172.20.1.131[49154]
Annotation: IP Transition Configuration endpoint
UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1
Endpoint: ncacn_ip_tcp:172.20.1.131[49154]
Annotation: AppInfo
UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1
Endpoint: ncacn_ip_tcp:172.20.1.131[49154]
Annotation: AppInfo
UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
Endpoint: ncacn_ip_tcp:172.20.1.131[49154]
UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1
Endpoint: ncacn_ip_tcp:172.20.1.131[49154]
Annotation: XactSrv service
UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1
Endpoint: ncacn_ip_tcp:172.20.1.131[49154]
Annotation: IKE/Authip API
UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1
Endpoint: ncacn_ip_tcp:172.20.1.131[49154]
Annotation: AppInfo

Port: 49155/tcp
UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
Endpoint: ncacn_ip_tcp:172.20.1.131[49155]
Port: 49156/tcp
UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
Endpoint: ncacn_ip_tcp:172.20.1.131[49156]
Named pipe : lsass
Win32 service or process : lsass.exe
Description : SAM access
Port: 49201/tcp
UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
Endpoint: ncacn_ip_tcp:172.20.1.131[49201]
Annotation: IPSec Policy agent endpoint
Named pipe : spoolss
Win32 service or process : spoolsv.exe
Description : Spooler service
UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1
Endpoint: ncacn_ip_tcp:172.20.1.131[49201]
Annotation: Remote Fw APIs
Note: DCE/RPC or MSRPC services running on this host locally were identified. Reporting this list is not enabled by default due to the possible large size of this list. See the script preferences to enable this reporting.
Impact:
An attacker may use this fact to gain more knowledge
about the remote host.
Solution:
Filter incoming traffic to this ports.
Summary:
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running
on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Base Score: 5.0
Family name: Windows
Category: infos

Summary: NOSUMMARY
Version: $Revision: 6319 $

High:

Apache HTTP Server < 2.4.38 HTTP/2 DoS Vulnerability (Windows)
Risk: High
Application: general
Port: 0
Protocol: tcp
ScriptID: 141965
Vulnerability Detection Result:
Installed version: 2.4.37
Fixed version: 2.4.38
Vulnerability Detection Method:
Checks if a vulnerable version is present on the target host.
Affected Software/OS:
Apache HTTP server version 2.4.37 and prior.
Summary:
By sending request bodies in a slow loris way to plain resources, the h2
stream for that request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 connections. A possible mitigation is to not enable the h2 protocol.
Solution:
Update to version 2.4.38 or later.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:P
References:
https://httpd.apache.org/security/vulnerabilities_24.html
CVSS Base Score: 5.0
Family name: Web Servers
Category: unknown

Version: $Revision: 13547 $

High:

http TRACE XSS attack
Risk: High
Application: https
Port: 443
Protocol: tcp
ScriptID: 11213
Vulnerability Detection Result:
The web server has the following HTTP methods enabled: TRACE
CVSS Base Vector:
AV:N/AC:M/Au:N/C:P/I:P/A:N
Insight:
It has been shown that web servers supporting this methods are
subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in
conjunction with various weaknesses in browsers.
Impact:
An attacker may use this flaw to trick your legitimate web users to give
him their credentials.
Affected Software/OS:
Web servers with enabled TRACE and/or TRACK methods.
Solution:
Disable the TRACE and TRACK methods in your web server configuration.
Please see the manual of your web server or the references for more information.
Summary:
Debugging functions are enabled on the remote web server.
The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK
are HTTP methods which are used to debug web server connections.
References:
http://www.kb.cert.org/vuls/id/288308
http://www.kb.cert.org/vuls/id/867593
http://httpd.apache.org/docs/current/de/mod/core.html#traceenable
https://www.owasp.org/index.php/Cross_Site_Tracing
CVSS Base Score: 5.8
Family name: Web application abuses
Category: infos

Summary: NOSUMMARY
Version: $Revision: 10828 $

High:

http TRACE XSS attack
Risk: High
Application: http
Port: 80
Protocol: tcp
ScriptID: 11213
Vulnerability Detection Result:
The web server has the following HTTP methods enabled: TRACE
Insight:
It has been shown that web servers supporting this methods are
subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in
conjunction with various weaknesses in browsers.
CVSS Base Vector:
AV:N/AC:M/Au:N/C:P/I:P/A:N
Solution:
Disable the TRACE and TRACK methods in your web server configuration.
Please see the manual of your web server or the references for more information.
Summary:
Debugging functions are enabled on the remote web server.
The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK
are HTTP methods which are used to debug web server connections.
Affected Software/OS:
Web servers with enabled TRACE and/or TRACK methods.
Impact:
An attacker may use this flaw to trick your legitimate web users to give
him their credentials.
References:
http://www.kb.cert.org/vuls/id/288308
http://www.kb.cert.org/vuls/id/867593
http://httpd.apache.org/docs/current/de/mod/core.html#traceenable
https://www.owasp.org/index.php/Cross_Site_Tracing
CVSS Base Score: 5.8
Family name: Web application abuses
Category: infos
Copyright: This script is Copyright (C) 2003 E-Soft Inc.
Summary: NOSUMMARY
Version: $Revision: 10828 $

High:

Apache HTTP Server < 2.4.38 mod_session_cookie Vulnerability (Windows)
Risk: High
Application: general
Port: 0
Protocol: tcp
ScriptID: 141963
Vulnerability Detection Result:
Installed version: 2.4.37
Fixed version: 2.4.38
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:P/A:N
Affected Software/OS:
Apache HTTP server version 2.4.37 and prior.
Vulnerability Detection Method:
Checks if a vulnerable version is present on the target host.
Summary:
In Apache HTTP Server mod_session checks the session expiry time before
decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.
Solution:
Update to version 2.4.38 or later.
References:
https://httpd.apache.org/security/vulnerabilities_24.html
CVSS Base Score: 5.0
Family name: Web Servers
Category: unknown

Version: $Revision: 13750 $

High:

Apache HTTP Server < 2.4.38 mod_session_cookie Vulnerability (Windows)
Risk: High
Application: general
Port: 0
Protocol: tcp
ScriptID: 141963
Vulnerability Detection Result:
Installed version: 2.4.37
Fixed version: 2.4.38
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:P/A:N
Solution:
Update to version 2.4.38 or later.
Summary:
In Apache HTTP Server mod_session checks the session expiry time before
decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.
Affected Software/OS:
Apache HTTP server version 2.4.37 and prior.
Vulnerability Detection Method:
Checks if a vulnerable version is present on the target host.
References:
https://httpd.apache.org/security/vulnerabilities_24.html
CVSS Base Score: 5.0
Family name: Web Servers
Category: unknown

Version: $Revision: 13750 $

High:

Apache HTTP Server < 2.4.39 mod_auth_digest Access Control Bypass Vulnerability (Windows)
Risk: High
Application: general
Port: 0
Protocol: tcp
ScriptID: 142221
Vulnerability Detection Result:
Installed version: 2.4.37
Fixed version: 2.4.39
CVSS Base Vector:
AV:N/AC:M/Au:S/C:P/I:P/A:P
Affected Software/OS:
Apache HTTP server version 2.4.38 and prior.
Vulnerability Detection Method:
Checks if a vulnerable version is present on the target host.
Solution:
Update to version 2.4.39 or later.
Summary:
In Apache HTTP Server, a race condition in mod_auth_digest when running in a
threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.
References:
https://httpd.apache.org/security/vulnerabilities_24.html
CVSS Base Score: 6.0
Family name: Web Servers
Category: unknown

Version: 2019-04-15T07:08:44+0000

High:

PHP 'PHP-FPM' Denial of Service Vulnerability (Windows)
Risk: High
Application: https
Port: 443
Protocol: tcp
ScriptID: 812519
Vulnerability Detection Result:
Installed version: 7.0.33
Fixed version: 7.1.20
Installation
path / port: 443/tcp
Solution:
Update to PHP 7.1.20, 7.2.8 or 7.3.0alpha3.
Summary:
This host is installed with PHP and is prone
to denial of service vulnerability.
Affected Software/OS:
PHP versions 5.x up to and including 5.6.36. All 7.0.x versions,
7.1.x before 7.1.20, 7.2.x before 7.2.8 and 7.3.x before 7.3.0alpha3 on Windows.
Vulnerability Detection Method:
Checks if a vulnerable version is present on the target host.
Impact:
Successfully exploitation will allow an
attackers to consume 100% of the CPU, and consume disk space with a large
volume of error logs, as demonstrated by an attack by a customer of a
shared-hosting facility.
Insight:
The flaw exist due to the php-fpm master
process restarts a child process in an endless loop when using program
execution functions with a non-blocking STDIN stream.
CVSS Base Vector:
AV:N/AC:L/Au:S/C:N/I:N/A:C
References:
https://bugs.php.net/bug.php?id=73342
https://bugs.php.net/bug.php?id=70185
https://github.com/php/php-src/pull/3287
https://www.futureweb.at/security/CVE-2015-9253
https://vuldb.com//?id.113566
CVSS Base Score: 6.8
Family name: Web application abuses
Category: infos
Copyright: Copyright (C) 2018 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 12762 $

High:

PHP 'PHP-FPM' Denial of Service Vulnerability (Windows)
Risk: High
Application: http
Port: 80
Protocol: tcp
ScriptID: 812519
Vulnerability Detection Result:
Installed version: 7.0.33
Fixed version: 7.1.20
Installation
path / port: 80/tcp
Solution:
Update to PHP 7.1.20, 7.2.8 or 7.3.0alpha3.
Summary:
This host is installed with PHP and is prone
to denial of service vulnerability.
Impact:
Successfully exploitation will allow an
attackers to consume 100% of the CPU, and consume disk space with a large
volume of error logs, as demonstrated by an attack by a customer of a
shared-hosting facility.
Affected Software/OS:
PHP versions 5.x up to and including 5.6.36. All 7.0.x versions,
7.1.x before 7.1.20, 7.2.x before 7.2.8 and 7.3.x before 7.3.0alpha3 on Windows.
Vulnerability Detection Method:
Checks if a vulnerable version is present on the target host.
Insight:
The flaw exist due to the php-fpm master
process restarts a child process in an endless loop when using program
execution functions with a non-blocking STDIN stream.
CVSS Base Vector:
AV:N/AC:L/Au:S/C:N/I:N/A:C
References:
https://bugs.php.net/bug.php?id=73342
https://bugs.php.net/bug.php?id=70185
https://github.com/php/php-src/pull/3287
https://www.futureweb.at/security/CVE-2015-9253
https://vuldb.com//?id.113566
CVSS Base Score: 6.8
Family name: Web application abuses
Category: infos
Copyright: Copyright (C) 2018 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 12762 $

High:

PHP Integer Overflow Vulnerability Aug18 (Windows)
Risk: High
Application: https
Port: 443
Protocol: tcp
ScriptID: 813598
Vulnerability Detection Result:
Installed version: 7.0.33
Fixed version: None
Installation
path / port: 443/tcp
Insight:
The flaw exists due to
mysqli_real_escape_string function in mysqli/mysqli_api.c file improperly handles long string.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:P/I:P/A:P
Summary:
This host is installed with PHP and is prone
to denial of service vulnerability.
Solution:
No known solution is available as of 13th May, 2019.
Information regarding this issue will be updated once solution details are available.
Impact:
Successful exploitation will allow attackers
to cause denial of service by performing integer overflow and therefore, crashing the application.
Vulnerability Detection Method:
Checks if a vulnerable version is present on the target host.
Affected Software/OS:
PHP versions 7.0.x through 7.1.15
References:
https://bugs.php.net/bug.php?id=74544
CVSS Base Score: 7.5
Family name: Web application abuses
Category: infos
Copyright: Copyright (C) 2018 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: 2019-05-13T06:06:12+0000

High:

PHP Integer Overflow Vulnerability Aug18 (Windows)
Risk: High
Application: http
Port: 80
Protocol: tcp
ScriptID: 813598
Vulnerability Detection Result:
Installed version: 7.0.33
Fixed version: None
Installation
path / port: 80/tcp
Impact:
Successful exploitation will allow attackers
to cause denial of service by performing integer overflow and therefore, crashing the application.
Vulnerability Detection Method:
Checks if a vulnerable version is present on the target host.
Affected Software/OS:
PHP versions 7.0.x through 7.1.15
Summary:
This host is installed with PHP and is prone
to denial of service vulnerability.
Solution:
No known solution is available as of 13th May, 2019.
Information regarding this issue will be updated once solution details are available.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:P/I:P/A:P
Insight:
The flaw exists due to
mysqli_real_escape_string function in mysqli/mysqli_api.c file improperly handles long string.
References:
https://bugs.php.net/bug.php?id=74544
CVSS Base Score: 7.5
Family name: Web application abuses
Category: infos
Copyright: Copyright (C) 2018 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: 2019-05-13T06:06:12+0000

High:

PHP Memory Disclosure Vulnerability (Windows)
Risk: High
Application: https
Port: 443
Protocol: tcp
ScriptID: 142047
Vulnerability Detection Result:
Installed version: 7.0.33
Fixed version: 7.1.26
Installation
path / port: 443/tcp
CVSS Base Vector:
AV:N/AC:L/Au:N/C:P/I:N/A:N
Affected Software/OS:
PHP version 7.x before 7.1.26, 7.2.x before 7.2.14 and 7.3.x before 7.3.2.
Vulnerability Detection Method:
Checks if a vulnerable version is present on the target host.
Solution:
Update to version 7.1.26, 7.2.14, 7.3.2 or later.
Summary:
dns_get_record misparses a DNS response, which can allow a hostile DNS server
to cause PHP to misuse memcpy, leading to read operations going past the buffer allocated for DNS data. This affects php_parserr in ext/standard/dns.c for DNS_CAA and DNS_ANY queries.
References:
https://bugs.php.net/bug.php?id=77369
CVSS Base Score: 5.0
Family name: Web application abuses
Category: unknown

Version: $Revision: 13857 $

High:

PHP Memory Disclosure Vulnerability (Windows)
Risk: High
Application: http
Port: 80
Protocol: tcp
ScriptID: 142047
Vulnerability Detection Result:
Installed version: 7.0.33
Fixed version: 7.1.26
Installation
path / port: 80/tcp
CVSS Base Vector:
AV:N/AC:L/Au:N/C:P/I:N/A:N
Affected Software/OS:
PHP version 7.x before 7.1.26, 7.2.x before 7.2.14 and 7.3.x before 7.3.2.
Vulnerability Detection Method:
Checks if a vulnerable version is present on the target host.
Summary:
dns_get_record misparses a DNS response, which can allow a hostile DNS server
to cause PHP to misuse memcpy, leading to read operations going past the buffer allocated for DNS data. This affects php_parserr in ext/standard/dns.c for DNS_CAA and DNS_ANY queries.
Solution:
Update to version 7.1.26, 7.2.14, 7.3.2 or later.
References:
https://bugs.php.net/bug.php?id=77369
CVSS Base Score: 5.0
Family name: Web application abuses
Category: unknown

Version: $Revision: 13857 $

High:

Apache HTTP Server < 2.4.39 mod_auth_digest Access Control Bypass Vulnerability (Windows)
Risk: High
Application: general
Port: 0
Protocol: tcp
ScriptID: 142221
Vulnerability Detection Result:
Installed version: 2.4.37
Fixed version: 2.4.39
CVSS Base Vector:
AV:N/AC:M/Au:S/C:P/I:P/A:P
Solution:
Update to version 2.4.39 or later.
Summary:
In Apache HTTP Server, a race condition in mod_auth_digest when running in a
threaded server could allow a user with valid credentials to authenticate using another username, bypassing
configured access control restrictions.
Affected Software/OS:
Apache HTTP server version 2.4.38 and prior.
Vulnerability Detection Method:
Checks if a vulnerable version is present on the target host.
References:
https://httpd.apache.org/security/vulnerabilities_24.html
CVSS Base Score: 6.0
Family name: Web Servers
Category: unknown
Copyright: This script is Copyright (C) 2019 Greenbone Networks GmbH
Version: 2019-04-15T07:08:44+0000

High:

PHP Multiple Vulnerabilities - Feb19 (Windows)
Risk: High
Application: https
Port: 443
Protocol: tcp
ScriptID: 142049
Vulnerability Detection Result:
Installed version: 7.0.33
Fixed version: 7.1.26
Installation
path / port: 443/tcp
CVSS Base Vector:
AV:N/AC:L/Au:N/C:P/I:P/A:P
Insight:
PHP is prone to multiple vulnerabilities:
- Invalid input to the function xmlrpc_decode() can lead to an invalid memory access (heap out of bounds read or read after free). This is related to xml_elem_parse_buf in ext/xmlrpc/libxmlrpc/xml_element.c. (CVE-2019-9020)
- A heap-based buffer over-read in PHAR reading functions in the PHAR extension may allow an attacker to read allocated or unallocated memory past the actual data when trying to parse the file name. (CVE-2019-9021)
- A number of heap-based buffer over-read instances are present in mbstring regular expression functions when supplied with invalid multibyte data. (CVE-2019-9023)
- xmlrpc_decode() can allow a hostile XMLRPC server to cause PHP to read memory outside of allocated areas (CVE-2019-9024)
Vulnerability Detection Method:
Checks if a vulnerable version is present on the target host.
Affected Software/OS:
PHP versions before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14 and
7.3.x before 7.3.1.
Summary:
PHP is prone to multiple vulnerabilities.
Solution:
Update to version 5.6.40, 7.1.16, 7.2.14, 7.3.1 or later.
References:
https://bugs.php.net/bug.php?id=77242
https://bugs.php.net/bug.php?id=77249
https://bugs.php.net/bug.php?id=77247
https://bugs.php.net/bug.php?id=77370
https://bugs.php.net/bug.php?id=77371
https://bugs.php.net/bug.php?id=77381
https://bugs.php.net/bug.php?id=77382
https://bugs.php.net/bug.php?id=77385
https://bugs.php.net/bug.php?id=77394
https://bugs.php.net/bug.php?id=77418
https://bugs.php.net/bug.php?id=77380
CVSS Base Score: 7.5
Family name: Web application abuses
Category: unknown

Version: $Revision: 13857 $

High:

PHP Multiple Vulnerabilities - Feb19 (Windows)
Risk: High
Application: http
Port: 80
Protocol: tcp
ScriptID: 142049
Vulnerability Detection Result:
Installed version: 7.0.33
Fixed version: 7.1.26
Installation
path / port: 80/tcp
Insight:
PHP is prone to multiple vulnerabilities:
- Invalid input to the function xmlrpc_decode() can lead to an invalid memory access (heap out of bounds read or read after free). This is related to xml_elem_parse_buf in ext/xmlrpc/libxmlrpc/xml_element.c. (CVE-2019-9020)
- A heap-based buffer over-read in PHAR reading functions in the PHAR extension may allow an attacker to read allocated or unallocated memory past the actual data when trying to parse the file name. (CVE-2019-9021)
- A number of heap-based buffer over-read instances are present in mbstring regular expression functions when supplied with invalid multibyte data. (CVE-2019-9023)
- xmlrpc_decode() can allow a hostile XMLRPC server to cause PHP to read memory outside of allocated areas (CVE-2019-9024)
CVSS Base Vector:
AV:N/AC:L/Au:N/C:P/I:P/A:P
Summary:
PHP is prone to multiple vulnerabilities.
Solution:
Update to version 5.6.40, 7.1.16, 7.2.14, 7.3.1 or later.
Affected Software/OS:
PHP versions before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14 and
7.3.x before 7.3.1.
Vulnerability Detection Method:
Checks if a vulnerable version is present on the target host.
References:
https://bugs.php.net/bug.php?id=77242
https://bugs.php.net/bug.php?id=77249
https://bugs.php.net/bug.php?id=77247
https://bugs.php.net/bug.php?id=77370
https://bugs.php.net/bug.php?id=77371
https://bugs.php.net/bug.php?id=77381
https://bugs.php.net/bug.php?id=77382
https://bugs.php.net/bug.php?id=77385
https://bugs.php.net/bug.php?id=77394
https://bugs.php.net/bug.php?id=77418
https://bugs.php.net/bug.php?id=77380
CVSS Base Score: 7.5
Family name: Web application abuses
Category: unknown

Version: $Revision: 13857 $

High:

PHP Multiple Vulnerabilities - Mar19 (Windows)
Risk: High
Application: https
Port: 443
Protocol: tcp
ScriptID: 142132
Vulnerability Detection Result:
Installed version: 7.0.33
Fixed version: 7.1.27
Installation
path / port: 443/tcp
Affected Software/OS:
PHP version 7.x before 7.1.27, 7.2.x before 7.2.16 and 7.3.x before 7.3.3.
Vulnerability Detection Method:
Checks if a vulnerable version is present on the target host.
Summary:
PHP is prone to multiple vulnerabilities.
Solution:
Update to version 7.1.27, 7.2.16, 7.3.3 or later.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:P/I:P/A:P
Insight:
PHP is prone to multiple vulnerabilities:
- Due to the way rename() across filesystems is implemented, it is possible that file being renamed is briefly available with wrong permissions while the rename is ongoing, thus enabling unauthorized users to access the data. (CVE-2019-9637)
- Uninitialized read in exif_process_IFD_in_MAKERNOTE because of mishandling the maker_note->offset relationship to value_len (CVE-2019-9638)
- Uninitialized read in exif_process_IFD_in_MAKERNOTE because of mishandling the data_len variable (CVE-2019-9639)
- Invalid Read in exif_process_SOFn (CVE-2019-9640)
- Uninitialized read in exif_process_IFD_in_TIFF (CVE-2019-9641)
References:
https://bugs.php.net/bug.php?id=77630
https://bugs.php.net/bug.php?id=77563
https://bugs.php.net/bug.php?id=77659
https://bugs.php.net/bug.php?id=77540
https://bugs.php.net/bug.php?id=77509
CVSS Base Score: 7.5
Family name: Web application abuses
Category: unknown

Version: 2019-04-12T12:22:59+0000

High:

PHP Multiple Vulnerabilities - Mar19 (Windows)
Risk: High
Application: http
Port: 80
Protocol: tcp
ScriptID: 142132
Vulnerability Detection Result:
Installed version: 7.0.33
Fixed version: 7.1.27
Installation
path / port: 80/tcp
CVSS Base Vector:
AV:N/AC:L/Au:N/C:P/I:P/A:P
Insight:
PHP is prone to multiple vulnerabilities:
- Due to the way rename() across filesystems is implemented, it is possible that file being renamed is briefly available with wrong permissions while the rename is ongoing, thus enabling unauthorized users to access the data. (CVE-2019-9637)
- Uninitialized read in exif_process_IFD_in_MAKERNOTE because of mishandling the maker_note->offset relationship to value_len (CVE-2019-9638)
- Uninitialized read in exif_process_IFD_in_MAKERNOTE because of mishandling the data_len variable (CVE-2019-9639)
- Invalid Read in exif_process_SOFn (CVE-2019-9640)
- Uninitialized read in exif_process_IFD_in_TIFF (CVE-2019-9641)
Affected Software/OS:
PHP version 7.x before 7.1.27, 7.2.x before 7.2.16 and 7.3.x before 7.3.3.
Vulnerability Detection Method:
Checks if a vulnerable version is present on the target host.
Summary:
PHP is prone to multiple vulnerabilities.
Solution:
Update to version 7.1.27, 7.2.16, 7.3.3 or later.
References:
https://bugs.php.net/bug.php?id=77630
https://bugs.php.net/bug.php?id=77563
https://bugs.php.net/bug.php?id=77659
https://bugs.php.net/bug.php?id=77540
https://bugs.php.net/bug.php?id=77509
CVSS Base Score: 7.5
Family name: Web application abuses
Category: unknown

Version: 2019-04-12T12:22:59+0000

High:

phpinfo() output accessible
Risk: High
Application: https
Port: 443
Protocol: tcp
ScriptID: 11229
Vulnerability Detection Result:
The following files are calling the function phpinfo() which disclose potentially sensitive information:
https://172.20.1.131/dashboard/phpinfo.php
CVSS Base Vector:
AV:N/AC:L/Au:N/C:P/I:P/A:P
Impact:
Some of the information that can be gathered from this file includes:
The username of the user running the PHP process, if it is a sudo user, the IP address of the host, the web server version, the system version (Unix, Linux, Windows, ...), and the root directory of the web server.
Summary:
Many PHP installation tutorials instruct the user to create
a file called phpinfo.php or similar containing the phpinfo() statement. Such a file is often
left back in the webserver directory.
Solution:
Delete the listed files or restrict access to them.
CVSS Base Score: 7.5
Family name: Web application abuses
Category: infos
Copyright: This script is Copyright (C) 2003 Randy Matz
Summary: NOSUMMARY
Version: $Revision: 11992 $

High:

phpinfo() output accessible
Risk: High
Application: http
Port: 80
Protocol: tcp
ScriptID: 11229
Vulnerability Detection Result:
The following files are calling the function phpinfo() which disclose potentially sensitive information:
http://172.20.1.131/dashboard/phpinfo.php
CVSS Base Vector:
AV:N/AC:L/Au:N/C:P/I:P/A:P
Impact:
Some of the information that can be gathered from this file includes:
The username of the user running the PHP process, if it is a sudo user, the IP address of the host, the web server version, the system version (Unix, Linux, Windows, ...), and the root directory of the web server.
Solution:
Delete the listed files or restrict access to them.
Summary:
Many PHP installation tutorials instruct the user to create
a file called phpinfo.php or similar containing the phpinfo() statement. Such a file is often
left back in the webserver directory.
CVSS Base Score: 7.5
Family name: Web application abuses
Category: infos
Copyright: This script is Copyright (C) 2003 Randy Matz
Summary: NOSUMMARY
Version: $Revision: 11992 $

High:

Apache HTTP Server < 2.4.39 mod_http2 DoS Vulnerability (Windows)
Risk: High
Application: general
Port: 0
Protocol: tcp
ScriptID: 142227
Vulnerability Detection Result:
Installed version: 2.4.37
Fixed version: 2.4.39
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:P
Affected Software/OS:
Apache HTTP server version 2.4.38 and prior.
Vulnerability Detection Method:
Checks if a vulnerable version is present on the target host.
Solution:
Update to version 2.4.39 or later.
Summary:
Using fuzzed network input, the http/2 request handling could be made to
access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.
References:
https://httpd.apache.org/security/vulnerabilities_24.html
CVSS Base Score: 5.0
Family name: Web Servers
Category: unknown

Version: 2019-04-08T15:50:06+0000

High:

Apache HTTP Server < 2.4.39 mod_http2 DoS Vulnerability (Windows)
Risk: High
Application: general
Port: 0
Protocol: tcp
ScriptID: 142227
Vulnerability Detection Result:
Installed version: 2.4.37
Fixed version: 2.4.39
Affected Software/OS:
Apache HTTP server version 2.4.38 and prior.
Vulnerability Detection Method:
Checks if a vulnerable version is present on the target host.
Solution:
Update to version 2.4.39 or later.
Summary:
Using fuzzed network input, the http/2 request handling could be made to
access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:P
References:
https://httpd.apache.org/security/vulnerabilities_24.html
CVSS Base Score: 5.0
Family name: Web Servers
Category: unknown

Version: 2019-04-08T15:50:06+0000

Medium:

Apache HTTP Server < 2.4.39 mod_http2 DoS Vulnerability (Windows)
Risk: Medium
Application: general
Port: 0
Protocol: tcp
ScriptID: 142225
Vulnerability Detection Result:
Installed version: 2.4.37
Fixed version: 2.4.39
CVSS Base Vector:
AV:N/AC:M/Au:S/C:N/I:P/A:P
Solution:
Update to version 2.4.39 or later.
Summary:
When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a
https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. A server that never enabled the h2 protocol or that only enabled it for https: and did not configure the '2Upgrade on' is unaffected by this.
Affected Software/OS:
Apache HTTP server version 2.4.38, 2.4.37, 2.4.35 and 2.4.34.
Vulnerability Detection Method:
Checks if a vulnerable version is present on the target host.
References:
https://httpd.apache.org/security/vulnerabilities_24.html
CVSS Base Score: 4.9
Family name: Web Servers
Category: unknown
Copyright: This script is Copyright (C) 2019 Greenbone Networks GmbH
Version: 2019-06-17T06:50:08+0000

Medium:

Apache HTTP Server < 2.4.39 mod_http2 DoS Vulnerability (Windows)
Risk: Medium
Application: general
Port: 0
Protocol: tcp
ScriptID: 142225
Vulnerability Detection Result:
Installed version: 2.4.37
Fixed version: 2.4.39
Summary:
When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a
https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. A server that never enabled the h2 protocol or that only enabled it for https: and did not configure the '2Upgrade on' is unaffected by this.
Solution:
Update to version 2.4.39 or later.
Vulnerability Detection Method:
Checks if a vulnerable version is present on the target host.
Affected Software/OS:
Apache HTTP server version 2.4.38, 2.4.37, 2.4.35 and 2.4.34.
CVSS Base Vector:
AV:N/AC:M/Au:S/C:N/I:P/A:P
References:
https://httpd.apache.org/security/vulnerabilities_24.html
CVSS Base Score: 4.9
Family name: Web Servers
Category: unknown
Copyright: This script is Copyright (C) 2019 Greenbone Networks GmbH
Version: 2019-06-17T06:50:08+0000

Medium:

SSL/TLS: Certificate Signed Using A Weak Signature Algorithm
Risk: Medium
Application: https
Port: 443
Protocol: tcp
ScriptID: 105880
Vulnerability Detection Result:
The following certificates are part of the certificate chain but using insecure signature algorithms:
Subject: CN=localhost
Signature Algorithm: sha1WithRSAEncryption
CVSS Base Vector:
AV:N/AC:H/Au:N/C:P/I:P/A:N
Insight:
The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)
Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting
web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints
needs to be passed comma-separated and case-insensitive:
Fingerprint1
or
fingerprint1,Fingerprint2
Vulnerability Detection Method:
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Summary:
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.
Solution:
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new
SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.
References:
https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/
CVSS Base Score: 4.0
Family name: SSL and TLS
Category: infos

Summary: NOSUMMARY
Version: $Revision: 11524 $

Medium:

FTP Unencrypted Cleartext Login
Risk: Medium
Application: ftp
Port: 21
Protocol: tcp
ScriptID: 108528
Vulnerability Detection Result:
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command. Response(s):
Anonymous sessions: 331 Password required for anonymous
Non-anonymous sessions: 331 Password required for openvas-vt
Summary:
The remote host is running a FTP service that allows cleartext logins over
unencrypted connections.
Solution:
Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see
the manual of the FTP service for more information.
Impact:
An attacker can uncover login names and passwords by sniffing traffic to the
FTP service.
Vulnerability Detection Method:
Tries to login to a non FTPS enabled FTP service without sending a
'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of
the 'AUTH TLS' command.
CVSS Base Vector:
AV:A/AC:L/Au:N/C:P/I:P/A:N
CVSS Base Score: 4.8
Family name: General
Category: unknown

Version: $Revision: 13611 $

Medium:

IMAP Unencrypted Cleartext Logins
Risk: Medium
Application: imap
Port: 143
Protocol: tcp
ScriptID: 15856
Vulnerability Detection Result:
The remote IMAP server accepts logins via the following cleartext authentication mechanisms over unencrypted connections:
AUTH=PLAIN
Impact:
An attacker can uncover user names and passwords by sniffing traffic to the IMAP
daemon if a less secure authentication mechanism (eg, LOGIN command, AUTH=PLAIN, AUTH=LOGIN) is used.
Summary:
The remote host is running an IMAP daemon that allows cleartext logins over
unencrypted connections.
NOTE: Valid credentials needs to given to the settings of 'Login configurations' OID: 1.3.6.1.4.1.25623.1.0.10870.
Solution:
Configure the remote server to always enforce encrypted connections via
SSL/TLS with the 'STARTTLS' command.
CVSS Base Vector:
AV:A/AC:L/Au:N/C:P/I:P/A:N
References:
OSVDB:3119
http://www.ietf.org/rfc/rfc2222.txt
http://www.ietf.org/rfc/rfc2595.txt
CVSS Base Score: 4.8
Family name: General
Category: infos
Copyright: This script is Copyright (C) 2004 George A. Theall
Summary: NOSUMMARY
Version: $Revision: 13463 $

Medium:

OpenSSL: 0-byte record padding oracle (CVE-2019-1559) (Windows)
Risk: Medium
Application: https
Port: 443
Protocol: tcp
ScriptID: 108555
Vulnerability Detection Result:
Installed version: 1.0.2p
Fixed version: 1.0.2r
Installation
path / port: 443/tcp
Insight:
If an application encounters a fatal protocol error and then calls
SSL_shutdown() twice (once to send a close_notify, and once to receive one) then OpenSSL can respond
differently to the calling application if a 0 byte record is received with invalid padding compared
to if a 0 byte record is received with an invalid MAC.
CVSS Base Vector:
AV:N/AC:M/Au:N/C:P/I:N/A:N
Solution:
Upgrade OpenSSL to version 1.0.2r or later. See the references for more details.
Summary:
This host is running OpenSSL and is prone
to a padding oracle attack.
Affected Software/OS:
OpenSSL versions 1.0.2-1.0.2q.
This issue does not impact OpenSSL 1.1.1 or 1.1.0.
Vulnerability Detection Method:
Checks if a vulnerable version is present
on the target host.
Impact:
If the application then behaves differently based on that in a way that
is detectable to the remote peer, then this amounts to a padding oracle that could be used to decrypt data.
In order for this to be exploitable 'non-stitched' ciphersuites must be in use. Stitched ciphersuites
are optimised implementations of certain commonly used ciphersuites. Also the application must call
SSL_shutdown() twice even if a protocol error has occurred (applications should not do this but some
do anyway). AEAD ciphersuites are not impacted.
References:
https://www.openssl.org/news/secadv/20190226.txt
https://github.com/RUB-NDS/TLS-Padding-Oracles#openssl-cve-2019-1559
CVSS Base Score: 4.3
Family name: General
Category: unknown

Version: $Revision: 14008 $

Medium:

Timing vulnerability in DSA signature generation (CVE-2018-0734) (Windows)
Risk: Medium
Application: https
Port: 443
Protocol: tcp
ScriptID: 112410
Vulnerability Detection Result:
Installed version: 1.0.2p
Fixed version: 1.0.2q-dev
Installation
path / port: 443/tcp
Affected Software/OS:
OpenSSL versions 1.1.0-1.1.0i, 1.1.1 and 1.0.2-1.0.2p.
Vulnerability Detection Method:
Checks if a vulnerable version is present
on the target host.
Summary:
This host is running OpenSSL and is prone
to an information disclosure vulnerability.
Solution:
Upgrade OpenSSL to version 1.1.0j-dev, 1.1.1a-dev, 1.0.2q-dev or manually apply the fixes via Github.
See the references for more details.
CVSS Base Vector:
AV:N/AC:M/Au:N/C:P/I:N/A:N
Insight:
The OpenSSL DSA signature algorithm has been shown to be vulnerable to a
timing side channel attack. An attacker could use variations in the signing
algorithm to recover the private key.
References:
https://www.openssl.org/news/secadv/20181030.txt
https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=43e6a58d4991a451daf4891ff05a48735df871ac
https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=8abfe72e8c1de1b95f50aa0d9134803b4d00070f
https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=ef11e19d1365eea2b1851e6f540a0bf365d303e7
CVSS Base Score: 4.3
Family name: General
Category: infos
Copyright: Copyright (C) 2018 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 13898 $

Medium:

POP3 Unencrypted Cleartext Logins
Risk: Medium
Application: pop-3
Port: 110
Protocol: tcp
ScriptID: 15855
Vulnerability Detection Result:
The remote POP3 server accepts logins via the following cleartext authentication mechanisms over unencrypted connections:
USER
Solution:
Configure the remote server to always enforce encrypted connections via
SSL/TLS with the 'STLS' command.
Summary:
The remote host is running a POP3 daemon that allows cleartext logins over
unencrypted connections.
NOTE: Depending on the POP3 server configuration valid credentials needs to be given to the settings of
'Login configurations' OID: 1.3.6.1.4.1.25623.1.0.10870.
Impact:
An attacker can uncover user names and passwords by sniffing traffic to the POP3
daemon if a less secure authentication mechanism (eg, USER command, AUTH PLAIN, AUTH LOGIN) is used.
CVSS Base Vector:
AV:A/AC:L/Au:N/C:P/I:P/A:N
References:
OSVDB:3119
http://www.ietf.org/rfc/rfc2222.txt
http://www.ietf.org/rfc/rfc2595.txt
CVSS Base Score: 4.8
Family name: General
Category: infos
Copyright: This script is Copyright (C) 2004 George A. Theall
Summary: NOSUMMARY
Version: $Revision: 13459 $

Low:

OpenSSL: Microarchitecture timing vulnerability in ECC scalar multiplication (CVE-2018-5407) (Windows)
Risk: Low
Application: https
Port: 443
Protocol: tcp
ScriptID: 108484
Vulnerability Detection Result:
Installed version: 1.0.2p
Fixed version: 1.0.2q
Installation
path / port: 443/tcp
Affected Software/OS:
OpenSSL versions 1.1.0-1.1.0h and 1.0.2-1.0.2p.
Vulnerability Detection Method:
Checks if a vulnerable version is present
on the target host.
Impact:
An attacker with sufficient access to mount local timing attacks
during ECDSA signature generation could recover the private key.
Solution:
Upgrade OpenSSL to version 1.0.2q, 1.1.0i or later. See the references for more details.
Summary:
This host is running OpenSSL and is prone
to an information disclosure vulnerability.
CVSS Base Vector:
AV:L/AC:M/Au:N/C:P/I:N/A:N
Insight:
OpenSSL ECC scalar multiplication, used in e.g. ECDSA and ECDH,
has been shown to be vulnerable to a microarchitecture timing side channel attack.
References:
https://www.openssl.org/news/secadv/20181112.txt
https://www.openssl.org/news/vulnerabilities.html
https://github.com/openssl/openssl/commit/aab7c770353b1dc4ba045938c8fb446dd1c4531e
https://github.com/openssl/openssl/commit/b18162a7c9bbfb57112459a4d6631fa258fd8c0cq
http://www.securityfocus.com/bid/105897
https://eprint.iacr.org/2018/1060.pdf
https://github.com/bbbrumley/portsmash
https://www.exploit-db.com/exploits/45785/
CVSS Base Score: 1.9
Family name: General
Category: unknown

Version: $Revision: 13898 $

Info:

SMB Remote Version Detection
Risk: Info
Application: microsoft-ds
Port: 445
Protocol: tcp
ScriptID: 807830
Vulnerability Detection Result:
SMBv1 and SMBv2 are enabled on remote target
Summary:
Detection of Server Message Block(SMB).
This script sends SMB Negotiation request and try to get the version from the response.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: Copyright (C) 2016 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: 2019-05-16T07:13:31+0000

Info:

SMB/CIFS Server Detection
Risk: Info
Application: microsoft-ds
Port: 445
Protocol: tcp
ScriptID: 11011
Vulnerability Detection Result:
A CIFS server is running on this port
Summary:
This script detects whether port 445 and 139 are open and if they are running a CIFS/SMB server.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Windows
Category: infos
Copyright: This script is Copyright (C) 2002 Renaud Deraison
Summary: NOSUMMARY
Version: $Revision: 13541 $

Info:

SMB/CIFS Server Detection
Risk: Info
Application: netbios-ssn
Port: 139
Protocol: tcp
ScriptID: 11011
Vulnerability Detection Result:
A SMB server is running on this port
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
This script detects whether port 445 and 139 are open and
if they are running a CIFS/SMB server.
CVSS Base Score: 0.0
Family name: Windows
Category: infos
Copyright: This script is Copyright (C) 2002 Renaud Deraison
Summary: NOSUMMARY
Version: $Revision: 13541 $

Info:

SMBv1 enabled (Remote Check)
Risk: Info
Application: microsoft-ds
Port: 445
Protocol: tcp
ScriptID: 140151
Vulnerability Detection Result:
SMBv1 is enabled for the SMB Server
Summary:
The host has enabled SMBv1 for the SMB Server.
Vulnerability Detection Method:
Checks if SMBv1 is enabled for the SMB Server based on the
information provided by the following VT:
- SMB Remote Version Detection (OID: 1.3.6.1.4.1.25623.1.0.807830).
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
References:
https://www.us-cert.gov/ncas/current-activity/2017/01/16/SMB-Security-Best-Practices
https://support.microsoft.com/en-us/kb/2696547
https://support.microsoft.com/en-us/kb/204279
CVSS Base Score: 0.0
Family name: Windows
Category: infos
Copyright: Copyright (C) 2017 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: 2019-05-20T06:24:13+0000

Info:

SMTP Missing Support For STARTTLS
Risk: Info
Application: smtp
Port: 25
Protocol: tcp
ScriptID: 105091
Vulnerability Detection Result:
The remote SMTP server does not support the 'STARTTLS' command.
Summary:
The remote SMTP server does not support the 'STARTTLS' command.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: This script is Copyright (C) 2014 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 13153 $

Info:

SMTP Server type and version
Risk: Info
Application: smtp
Port: 25
Protocol: tcp
ScriptID: 10263
Vulnerability Detection Result:
Remote SMTP server banner:
220 localhost ESMTP server ready.
The remote SMTP server is announcing the following available ESMTP commands (EHLO response) via an unencrypted connection:
HELP, SIZE 0, TIME
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
This detects the SMTP Server's type and version by connecting to
the server and processing the buffer received.
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: This script is Copyright (C) 1999 SecuriTeam
Summary: NOSUMMARY
Version: $Revision: 14004 $

Info:

SSH Protocol Algorithms Supported
Risk: Info
Application: ssh
Port: 22
Protocol: tcp
ScriptID: 105565
Vulnerability Detection Result:
The following options are supported by the remote ssh service:
kex_algorithms:
curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-1.3.132.0.10,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group15-sha512,diffie-hellman-group14-sha256,diffie-hellman-group14-sha1,ext-info-s
server_host_key_algorithms:
rsa-sha2-512,rsa-sha2-256,ssh-rsa,ecdsa-sha2-nistp384
encryption_algorithms_client_to_server:
aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr,3des-ctr
encryption_algorithms_server_to_client:
aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr,3des-ctr
mac_algorithms_client_to_server:
hmac-sha2-256,hmac-sha1
mac_algorithms_server_to_client:
hmac-sha2-256,hmac-sha1
compression_algorithms_client_to_server:
zlib,none
compression_algorithms_server_to_client:
zlib,none
Summary:
This script detects which algorithms and languages are supported by the remote SSH Service
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Service detection
Category: infos

Summary: NOSUMMARY
Version: $Revision: 13581 $

Info:

SSH Protocol Versions Supported
Risk: Info
Application: ssh
Port: 22
Protocol: tcp
ScriptID: 100259
Vulnerability Detection Result:
The remote SSH Server supports the following SSH Protocol Versions:
2.0
SSHv2 Fingerprint(s):
ssh-rsa: 03:2c:15:69:8a:e1:1f:c0:f2:3f:db:66:5b:01:a0:f3
Note: The remote SSH service is accepting the non-existent SSH Protocol Version 0.12. Because of this behavior it is not possible to fingerprint the exact supported SSH Protocol Version. Based on this support for SSH Protocol Version 2.0 only is assumed.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
Identification of SSH protocol versions supported by the remote
SSH Server. Also reads the corresponding fingerprints from the service.
The following versions are tried: 1.33, 1.5, 1.99 and 2.0
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: This script is Copyright (C) 2009 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 13594 $

Info:

SSH Server type and version
Risk: Info
Application: ssh
Port: 22
Protocol: tcp
ScriptID: 10267
Vulnerability Detection Result:
Remote SSH server banner: SSH-2.0-8.38 FlowSsh: Bitvise SSH Server (WinSSHD) 8.39: free only for personal non-commercial use
Remote SSH supported authentication: password,publickey,keyboard-interactive
Remote SSH text/login banner: (not available)
This is probably:
- Bitvise SSH Server
Concluded from remote connection attempt with credentials:
Login: OpenVAS-VT
Password: OpenVAS-VT
Summary:
This detects the SSH Server's type and version by connecting to the server
and processing the buffer received.
This information gives potential attackers additional information about the system they are attacking.
Versions and Types should be omitted where possible.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Product detection
Category: infos

Summary: NOSUMMARY
Version: 2019-06-05T03:32:14+0000

Info:

SSL/TLS: Certificate - Self-Signed Certificate Detection
Risk: Info
Application: https
Port: 443
Protocol: tcp
ScriptID: 103140
Vulnerability Detection Result:
The certificate of the remote service is self signed.
Certificate details:
subject ...: CN=localhost
subject alternative names (SAN):
None
issued by .: CN=localhost
serial ....: 00B5C752C98781B503
valid from : 2009-11-10 23:48:47 UTC
valid until: 2019-11-08 23:48:47 UTC
fingerprint (SHA-1): B0238C547A905BFA119C4E8BACCAEACF36491FF6
fingerprint (SHA-256): 016973380C0F1DF00BD9593ED8D5EFA3706CD6DF7993F6141272B80522ACDD23
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
The SSL/TLS certificate on this port is self-signed.
References:
http://en.wikipedia.org/wiki/Self-signed_certificate
CVSS Base Score: 0.0
Family name: SSL and TLS
Category: infos
Copyright: This script is Copyright (C) 2011 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 8981 $

Info:

SSL/TLS: Collect and Report Certificate Details
Risk: Info
Application: https
Port: 443
Protocol: tcp
ScriptID: 103692
Vulnerability Detection Result:
The following certificate details of the remote service were collected.
Certificate details:
subject ...: CN=localhost
subject alternative names (SAN):
None
issued by .: CN=localhost
serial ....: 00B5C752C98781B503
valid from : 2009-11-10 23:48:47 UTC
valid until: 2019-11-08 23:48:47 UTC
fingerprint (SHA-1): B0238C547A905BFA119C4E8BACCAEACF36491FF6
fingerprint (SHA-256): 016973380C0F1DF00BD9593ED8D5EFA3706CD6DF7993F6141272B80522ACDD23
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
This script collects and reports the details of all SSL/TLS certificates.
This data will be used by other tests to verify server certificates.
CVSS Base Score: 0.0
Family name: SSL and TLS
Category: infos
Copyright: Copyright 2013 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: 2019-04-04T13:38:03+0000

Info:

SSL/TLS: HTTP Public Key Pinning (HPKP) Missing
Risk: Info
Application: https
Port: 443
Protocol: tcp
ScriptID: 108247
Vulnerability Detection Result:
The remote web server is not enforcing HPKP.
HTTP-Banner:
HTTP/1.1 302 Found
Date: ***replaced***
Server: Apache/2.4.37 (Win32) OpenSSL/1.0.2p PHP/7.0.33
X-Powered-By: PHP/7.0.33
Location: https://172.20.1.131/dashboard/
Content-Length: ***replaced***
Connection: close
Content-Type: text/html; charset=UTF-8

CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Solution:
Enable HPKP or add / configure the required directives correctly following the guides linked in the references.
Summary:
The remote web server is not enforcing HPKP.
References:
https://www.owasp.org/index.php/OWASP_Secure_Headers_Project
https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#hpkp
https://tools.ietf.org/html/rfc7469
https://securityheaders.io/
CVSS Base Score: 0.0
Family name: SSL and TLS
Category: infos
Copyright: This script is Copyright (C) 2017 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 7391 $

Info:

SSL/TLS: HTTP Strict Transport Security (HSTS) Missing
Risk: Info
Application: https
Port: 443
Protocol: tcp
ScriptID: 105879
Vulnerability Detection Result:
The remote web server is not enforcing HSTS.
HTTP-Banner:
HTTP/1.1 302 Found
Date: ***replaced***
Server: Apache/2.4.37 (Win32) OpenSSL/1.0.2p PHP/7.0.33
X-Powered-By: PHP/7.0.33
Location: https://172.20.1.131/dashboard/
Content-Length: ***replaced***
Connection: close
Content-Type: text/html; charset=UTF-8

Solution:
Enable HSTS or add / configure the required directives correctly following the guides linked in the references.
Summary:
The remote web server is not enforcing HSTS.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
References:
https://www.owasp.org/index.php/OWASP_Secure_Headers_Project
https://www.owasp.org/index.php/HTTP_Strict_Transport_Security_Cheat_Sheet
https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#hsts
https://tools.ietf.org/html/rfc6797
https://securityheaders.io/
CVSS Base Score: 0.0
Family name: SSL and TLS
Category: infos

Summary: NOSUMMARY
Version: $Revision: 7391 $

Info:

SSL/TLS: NPN / ALPN Extension and Protocol Support Detection
Risk: Info
Application: https
Port: 443
Protocol: tcp
ScriptID: 108099
Vulnerability Detection Result:
The remote service advertises support for the following Network Protocol(s) via the ALPN extension:
SSL/TLS Protocol:Network Protocol
TLSv1.0:HTTP/1.1
TLSv1.1:HTTP/1.1
TLSv1.2:HTTP/1.1
Summary:
This routine identifies services supporting the following extensions to TLS:
- Application-Layer Protocol Negotiation (ALPN)
- Next Protocol Negotiation (NPN).
Based on the availability of this extensions the supported Network Protocols by this service are gathered and reported.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
References:
https://tools.ietf.org/html/rfc7301
https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04
CVSS Base Score: 0.0
Family name: SSL and TLS
Category: infos
Copyright: Copyright (c) 2017 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 11638 $

Info:

Traceroute
Risk: Info
Application: general
Port: 0
Protocol: tcp
ScriptID: 51662
Vulnerability Detection Result:
Here is the route from 172.20.1.127 to 172.20.1.131:
172.20.1.127
?
Summary:
A traceroute from the scanning server to the target system was
conducted. This traceroute is provided primarily for informational value only. In the vast
majority of cases, it does not represent a vulnerability. However, if the displayed traceroute
contains any private addresses that should not have been publicly visible, then you have an
issue you need to correct.
Solution:
Block unwanted packets from escaping your network.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: General
Category: infos

Summary: NOSUMMARY
Version: $Revision: 10411 $

Info:

Unknown OS and Service Banner Reporting
Risk: Info
Application: general
Port: 0
Protocol: tcp
ScriptID: 108441
Vulnerability Detection Result:
Unknown banners have been collected which might help to identify the OS running on this host. If these banners containing information about the host OS please report the following information to https://community.greenbone.net/c/vulnerability-tests:
Banner: SSH-2.0-8.38 FlowSsh: Bitvise SSH Server (WinSSHD) 8.39: free only for personal non-commercial use
Identified from: SSH banner on port 22/tcp
Banner: +OK <52210945.30029@localhost>, POP3 server ready.
Identified from: POP3 banner on port 110/tcp
Banner: * OK localhost IMAP4rev1 Mercury/32 v4.62 server ready.
Identified from: IMAP banner on port 143/tcp
Banner: 220 localhost ESMTP server ready.
Identified from: SMTP banner on port 25/tcp
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
This NVT consolidates and reports the information collected by
the following NVTs:
- Collect banner of unknown services (OID: 1.3.6.1.4.1.25623.1.0.11154)
- Service Detection (unknown) with nmap (OID: 1.3.6.1.4.1.25623.1.0.66286)
- Service Detection (wrapped) with nmap (OID: 1.3.6.1.4.1.25623.1.0.108525)
- OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)
If you know any of the information reported here, please send the full output to
the referenced community portal.
References:
https://community.greenbone.net/c/vulnerability-tests
CVSS Base Score: 0.0
Family name: Service detection
Category: infos

Summary: NOSUMMARY
Version: $Revision: 12934 $

Info:

Unknown OS and Service Banner Reporting
Risk: Info
Application: pop3pw
Port: 106
Protocol: tcp
ScriptID: 108441
Vulnerability Detection Result:
An unknown service is running on this port. If you know this service, please report the following information to https://community.greenbone.net/c/vulnerability-tests:
Method: spontaneous
0x00: 32 30 30 20 6C 6F 63 61 6C 68 6F 73 74 20 4D 65 200 localhost Me
0x10: 72 63 75 72 79 57 20 50 6F 70 50 61 73 73 20 73 rcuryW PopPass s
0x20: 65 72 76 65 72 20 72 65 61 64 79 2E 0D 0A erver ready...
Nmap service detection (unknown) result for this port: pop3pw
Summary:
This NVT consolidates and reports the information collected by
the following NVTs:
- Collect banner of unknown services (OID: 1.3.6.1.4.1.25623.1.0.11154)
- Service Detection (unknown) with nmap (OID: 1.3.6.1.4.1.25623.1.0.66286)
- Service Detection (wrapped) with nmap (OID: 1.3.6.1.4.1.25623.1.0.108525)
- OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)
If you know any of the information reported here, please send the full output to
the referenced community portal.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
References:
https://community.greenbone.net/c/vulnerability-tests
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: Copyright (C) 2018 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 12934 $

Info:

XAMPP Version Detection
Risk: Info
Application: https
Port: 443
Protocol: tcp
ScriptID: 900526
Vulnerability Detection Result:
Detected XAMPP
Version: 7.0.33
Location: /dashboard
CPE: cpe:/a:apachefriends:xampp:7.0.33
Concluded from version/product identification result:
<h2>Welcome to XAMPP for Windows 7.0.33</h2>
Concluded from version/product identification location:
https://172.20.1.131/dashboard
Summary:
This script finds the installed XAMPP
version and saves the version in KB.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Product detection
Category: infos
Copyright: Copyright (C) 2009 SecPod
Summary: NOSUMMARY
Version: $Revision: 8141 $

Info:

XAMPP Version Detection
Risk: Info
Application: http
Port: 80
Protocol: tcp
ScriptID: 900526
Vulnerability Detection Result:
Detected XAMPP
Version: 7.0.33
Location: /dashboard
CPE: cpe:/a:apachefriends:xampp:7.0.33
Concluded from version/product identification result:
<h2>Welcome to XAMPP for Windows 7.0.33</h2>
Concluded from version/product identification location:
http://172.20.1.131/dashboard
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
This script finds the installed XAMPP
version and saves the version in KB.
CVSS Base Score: 0.0
Family name: Product detection
Category: infos
Copyright: Copyright (C) 2009 SecPod
Summary: NOSUMMARY
Version: $Revision: 8141 $

Info:

Apache Web Server Version Detection
Risk: Info
Application: https
Port: 443
Protocol: tcp
ScriptID: 900498
Vulnerability Detection Result:
Detected Apache
Version: 2.4.37
Location: 443/tcp
CPE: cpe:/a:apache:http_server:2.4.37
Concluded from version/product identification result:
Server: Apache/2.4.37
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
Detects the installed version of Apache Web Server
The script detects the version of Apache HTTP Server on remote host and sets the KB.
CVSS Base Score: 0.0
Family name: Product detection
Category: infos
Copyright: Copyright (C) 2009 SecPod
Summary: NOSUMMARY
Version: $Revision: 10290 $

Info:

Apache Web Server Version Detection
Risk: Info
Application: http
Port: 80
Protocol: tcp
ScriptID: 900498
Vulnerability Detection Result:
Detected Apache
Version: 2.4.37
Location: 80/tcp
CPE: cpe:/a:apache:http_server:2.4.37
Concluded from version/product identification result:
Server: Apache/2.4.37
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
Detects the installed version of Apache Web Server
The script detects the version of Apache HTTP Server on remote host and sets the KB.
CVSS Base Score: 0.0
Family name: Product detection
Category: infos
Copyright: Copyright (C) 2009 SecPod
Summary: NOSUMMARY
Version: $Revision: 10290 $

Info:

Bitvise SSH Server Detection
Risk: Info
Application: ssh
Port: 22
Protocol: tcp
ScriptID: 813383
Vulnerability Detection Result:
Detected Bitvise SSH Server
Version: 8.39
Location: 22/tcp
CPE: cpe:/a:bitvise:winsshd:8.39
Concluded from version/product identification result:
SSH-2.0-8.38 FlowSsh: Bitvise SSH Server (WinSSHD) 8.39: free only for personal non-commercial use
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
Detection of running version of
Bitvise SSH Server.
This script sends connection request and try to ensure the presence of
Bitvise SSH Server.
CVSS Base Score: 0.0
Family name: Product detection
Category: infos

Summary: NOSUMMARY
Version: $Revision: 13576 $

Info:

CGI Scanning Consolidation
Risk: Info
Application: https
Port: 443
Protocol: tcp
ScriptID: 111038
Vulnerability Detection Result:
The Hostname/IP "172.20.1.131" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable generic web application scanning" option within the "Global variable settings" of the scan config in use.
Requests to this service are done via HTTP/1.1.
This service seems to be able to host PHP scripts.
This service seems to be NOT able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 9.0.3)" was used to access the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI scanning. You can enable this again with the "Add historic /scripts and /cgi-bin to directories for CGI scanning" option within the "Global variable settings" of the scan config in use.
The following directories were used for CGI scanning:
https://172.20.1.131/
https://172.20.1.131/cgi-bin
https://172.20.1.131/dashboard
https://172.20.1.131/dashboard/docs
https://172.20.1.131/error
https://172.20.1.131/xampp
While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards
The following directories were excluded from CGI scanning because the "Regex pattern to exclude directories from CGI scanning" setting of the NVT "Global variable settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was: "/(index\.php|image|img|css|js$|js/|javascript|style|theme|icon|jquery|graphic|grafik|picture|bilder|thumbnail|media/|skins?/)"
https://172.20.1.131/dashboard/docs/images
https://172.20.1.131/dashboard/docs/images/access-phpmyadmin-remotely
https://172.20.1.131/dashboard/docs/images/activate-use-xdebug
https://172.20.1.131/dashboard/docs/images/auto-start-xampp
https://172.20.1.131/dashboard/docs/images/backup-restore-mysql
https://172.20.1.131/dashboard/docs/images/configure-use-tomcat
https://172.20.1.131/dashboard/docs/images/configure-vhosts
https://172.20.1.131/dashboard/docs/images/configure-wildcard-subdomains
https://172.20.1.131/dashboard/docs/images/create-framework-project-zf1
https://172.20.1.131/dashboard/docs/images/create-framework-project-zf2
https://172.20.1.131/dashboard/docs/images/deploy-git-app
https://172.20.1.131/dashboard/docs/images/install-wordpress
https://172.20.1.131/dashboard/docs/images/reset-mysql-password
https://172.20.1.131/dashboard/docs/images/send-mail
https://172.20.1.131/dashboard/docs/images/transfer-files-ftp
https://172.20.1.131/dashboard/docs/images/troubleshoot-apache
https://172.20.1.131/dashboard/docs/images/use-different-php-version
https://172.20.1.131/dashboard/docs/images/use-php-fcgi
https://172.20.1.131/dashboard/docs/images/use-sqlite
https://172.20.1.131/dashboard/images
https://172.20.1.131/dashboard/images/screenshots

https://172.20.1.131/dashboard/javascripts
https://172.20.1.131/dashboard/stylesheets
https://172.20.1.131/icons
https://172.20.1.131/img
Directory index found at:
https://172.20.1.131/dashboard/docs/
https://172.20.1.131/dashboard/docs/images/
https://172.20.1.131/dashboard/docs/images/access-phpmyadmin-remotely/
https://172.20.1.131/dashboard/docs/images/activate-use-xdebug/
https://172.20.1.131/dashboard/docs/images/auto-start-xampp/
https://172.20.1.131/dashboard/docs/images/backup-restore-mysql/
https://172.20.1.131/dashboard/docs/images/configure-use-tomcat/
https://172.20.1.131/dashboard/docs/images/configure-vhosts/
https://172.20.1.131/dashboard/docs/images/configure-wildcard-subdomains/
https://172.20.1.131/dashboard/docs/images/create-framework-project-zf1/
https://172.20.1.131/dashboard/docs/images/create-framework-project-zf2/
https://172.20.1.131/dashboard/docs/images/deploy-git-app/
https://172.20.1.131/dashboard/docs/images/install-wordpress/
https://172.20.1.131/dashboard/docs/images/reset-mysql-password/
https://172.20.1.131/dashboard/docs/images/send-mail/
https://172.20.1.131/dashboard/docs/images/transfer-files-ftp/
https://172.20.1.131/dashboard/docs/images/troubleshoot-apache/
https://172.20.1.131/dashboard/docs/images/use-different-php-version/
https://172.20.1.131/dashboard/docs/images/use-php-fcgi/
https://172.20.1.131/dashboard/docs/images/use-sqlite/
https://172.20.1.131/xampp/
Extraneous phpinfo() script found at:
https://172.20.1.131/dashboard/phpinfo.php
The "Number of pages to mirror" setting (Current: 200) of the NVT "Web mirroring" (OID: 1.3.6.1.4.1.25623.1.0.10662) was reached. Raising this limit allows to mirror this host more thoroughly but might increase the scanning time.
The following CGIs were discovered:
Syntax : cginame (arguments [default value])
https://172.20.1.131/dashboard/docs/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
https://172.20.1.131/dashboard/docs/images/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
https://172.20.1.131/dashboard/docs/images/access-phpmyadmin-remotely/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
https://172.20.1.131/dashboard/docs/images/activate-use-xdebug/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
https://172.20.1.131/dashboard/docs/images/auto-start-xampp/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
https://172.20.1.131/dashboard/docs/images/backup-restore-mysql/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
https://172.20.1.131/dashboard/docs/images/configure-use-tomcat/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
https://172.20.1.131/dashboard/docs/images/configure-vhosts/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
https://172.20.1.131/dashboard/docs/images/configure-wildcard-subdomains/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
https://172.20.1.131/dashboard/docs/images/create-framework-project-zf1/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
https://172.20.1.131/dashboard/docs/images/create-framework-project-zf2/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
https://172.20.1.131/dashboard/docs/images/deploy-git-app/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
https://172.20.1.131/dashboard/docs/images/install-wordpress/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
https://172.20.1.131/dashboard/docs/images/reset-mysql-password/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
https://172.20.1.131/dashboard/docs/images/send-mail/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
https://172.20.1.131/dashboard/docs/images/transfer-files-ftp/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])

https://172.20.1.131/dashboard/docs/images/troubleshoot-apache/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
https://172.20.1.131/dashboard/docs/images/use-different-php-version/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A]
)
https://172.20.1.131/dashboard/docs/images/use-php-fcgi/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
https://172.20.1.131/dashboard/docs/images/use-sqlite/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
https://172.20.1.131/xampp/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
Summary:
The script consolidates various information for CGI scanning.
This information is based on the following scripts / settings:
- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use
- The configured 'Enable CGI scanning', 'Enable generic web application scanning' and
'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the
'Global variable settings' of the scan config in use
If you think any of this information is wrong please report it to the referenced community portal.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
References:
https://community.greenbone.net/c/vulnerability-tests
CVSS Base Score: 0.0
Family name: Web application abuses
Category: infos
Copyright: This script is Copyright (C) 2015 SCHUTZWERK GmbH
Summary: NOSUMMARY
Version: $Revision: 13679 $

Info:

CGI Scanning Consolidation
Risk: Info
Application: http
Port: 80
Protocol: tcp
ScriptID: 111038
Vulnerability Detection Result:
The Hostname/IP "172.20.1.131" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable generic web application scanning" option within the "Global variable settings" of the scan config in use.
Requests to this service are done via HTTP/1.1.
This service seems to be able to host PHP scripts.
This service seems to be NOT able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 9.0.3)" was used to access the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI scanning. You can enable this again with the "Add historic /scripts and /cgi-bin to directories for CGI scanning" option within the "Global variable settings" of the scan config in use.
The following directories were used for CGI scanning:
http://172.20.1.131/
http://172.20.1.131/cgi-bin
http://172.20.1.131/dashboard
http://172.20.1.131/dashboard/docs
http://172.20.1.131/error
http://172.20.1.131/xampp
While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards
The following directories were excluded from CGI scanning because the "Regex pattern to exclude directories from CGI scanning" setting of the NVT "Global variable settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was: "/(index\.php|image|img|css|js$|js/|javascript|style|theme|icon|jquery|graphic|grafik|picture|bilder|thumbnail|media/|skins?/)"
http://172.20.1.131/dashboard/docs/images
http://172.20.1.131/dashboard/docs/images/access-phpmyadmin-remotely
http://172.20.1.131/dashboard/docs/images/activate-use-xdebug
http://172.20.1.131/dashboard/docs/images/auto-start-xampp
http://172.20.1.131/dashboard/docs/images/backup-restore-mysql
http://172.20.1.131/dashboard/docs/images/configure-use-tomcat
http://172.20.1.131/dashboard/docs/images/configure-vhosts
http://172.20.1.131/dashboard/docs/images/configure-wildcard-subdomains
http://172.20.1.131/dashboard/docs/images/create-framework-project-zf1
http://172.20.1.131/dashboard/docs/images/create-framework-project-zf2
http://172.20.1.131/dashboard/docs/images/deploy-git-app
http://172.20.1.131/dashboard/docs/images/install-wordpress
http://172.20.1.131/dashboard/docs/images/reset-mysql-password
http://172.20.1.131/dashboard/docs/images/send-mail
http://172.20.1.131/dashboard/docs/images/transfer-files-ftp
http://172.20.1.131/dashboard/docs/images/troubleshoot-apache
http://172.20.1.131/dashboard/docs/images/use-different-php-version
http://172.20.1.131/dashboard/docs/images/use-php-fcgi
http://172.20.1.131/dashboard/docs/images/use-sqlite
http://172.20.1.131/dashboard/images
http://172.20.1.131/dashboard/images/screenshots

http://172.20.1.131/dashboard/javascripts
http://172.20.1.131/dashboard/stylesheets
http://172.20.1.131/icons
http://172.20.1.131/img
Directory index found at:
http://172.20.1.131/dashboard/docs/
http://172.20.1.131/dashboard/docs/images/
http://172.20.1.131/dashboard/docs/images/access-phpmyadmin-remotely/
http://172.20.1.131/dashboard/docs/images/activate-use-xdebug/
http://172.20.1.131/dashboard/docs/images/auto-start-xampp/
http://172.20.1.131/dashboard/docs/images/backup-restore-mysql/
http://172.20.1.131/dashboard/docs/images/configure-use-tomcat/
http://172.20.1.131/dashboard/docs/images/configure-vhosts/
http://172.20.1.131/dashboard/docs/images/configure-wildcard-subdomains/
http://172.20.1.131/dashboard/docs/images/create-framework-project-zf1/
http://172.20.1.131/dashboard/docs/images/create-framework-project-zf2/
http://172.20.1.131/dashboard/docs/images/deploy-git-app/
http://172.20.1.131/dashboard/docs/images/install-wordpress/
http://172.20.1.131/dashboard/docs/images/reset-mysql-password/
http://172.20.1.131/dashboard/docs/images/send-mail/
http://172.20.1.131/dashboard/docs/images/transfer-files-ftp/
http://172.20.1.131/dashboard/docs/images/troubleshoot-apache/
http://172.20.1.131/dashboard/docs/images/use-different-php-version/
http://172.20.1.131/dashboard/docs/images/use-php-fcgi/
http://172.20.1.131/dashboard/docs/images/use-sqlite/
http://172.20.1.131/xampp/
Extraneous phpinfo() script found at:
http://172.20.1.131/dashboard/phpinfo.php
The "Number of pages to mirror" setting (Current: 200) of the NVT "Web mirroring" (OID: 1.3.6.1.4.1.25623.1.0.10662) was reached. Raising this limit allows to mirror this host more thoroughly but might increase the scanning time.
The following CGIs were discovered:
Syntax : cginame (arguments [default value])
http://172.20.1.131/dashboard/docs/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://172.20.1.131/dashboard/docs/images/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://172.20.1.131/dashboard/docs/images/access-phpmyadmin-remotely/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://172.20.1.131/dashboard/docs/images/activate-use-xdebug/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://172.20.1.131/dashboard/docs/images/auto-start-xampp/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://172.20.1.131/dashboard/docs/images/backup-restore-mysql/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://172.20.1.131/dashboard/docs/images/configure-use-tomcat/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://172.20.1.131/dashboard/docs/images/configure-vhosts/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://172.20.1.131/dashboard/docs/images/configure-wildcard-subdomains/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://172.20.1.131/dashboard/docs/images/create-framework-project-zf1/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://172.20.1.131/dashboard/docs/images/create-framework-project-zf2/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://172.20.1.131/dashboard/docs/images/deploy-git-app/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://172.20.1.131/dashboard/docs/images/install-wordpress/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://172.20.1.131/dashboard/docs/images/reset-mysql-password/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://172.20.1.131/dashboard/docs/images/send-mail/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://172.20.1.131/dashboard/docs/images/transfer-files-ftp/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])

http://172.20.1.131/dashboard/docs/images/troubleshoot-apache/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://172.20.1.131/dashboard/docs/images/use-different-php-version/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://172.20.1.131/dashboard/docs/images/use-php-fcgi/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://172.20.1.131/dashboard/docs/images/use-sqlite/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
http://172.20.1.131/xampp/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A])
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
The script consolidates various information for CGI scanning.
This information is based on the following scripts / settings:
- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use
- The configured 'Enable CGI scanning', 'Enable generic web application scanning' and
'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the
'Global variable settings' of the scan config in use
If you think any of this information is wrong please report it to the referenced community portal.
References:
https://community.greenbone.net/c/vulnerability-tests
CVSS Base Score: 0.0
Family name: Web application abuses
Category: infos
Copyright: This script is Copyright (C) 2015 SCHUTZWERK GmbH
Summary: NOSUMMARY
Version: $Revision: 13679 $

Info:

CPE Inventory
Risk: Info
Application: general
Port: 0
Protocol: CPE-T
ScriptID: 810002
Vulnerability Detection Result:
172.20.1.131|cpe:/a:apache:http_server:2.4.37
172.20.1.131|cpe:/a:apachefriends:xampp:7.0.33
172.20.1.131|cpe:/a:bitvise:winsshd:8.39
172.20.1.131|cpe:/a:filezilla:filezilla_server:0.9.41
172.20.1.131|cpe:/a:jquery:jquery:1.10.2
172.20.1.131|cpe:/a:mariadb:mariadb
172.20.1.131|cpe:/a:openssl:openssl:1.0.2p
172.20.1.131|cpe:/a:php:php:7.0.33
172.20.1.131|cpe:/o:microsoft:windows
Summary:
This routine uses information collected by other routines about
CPE identities of operating systems, services and
applications detected during the scan.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
References:
http://cpe.mitre.org/
CVSS Base Score: 0.0
Family name: Service detection
Category: end

Summary: NOSUMMARY
Version: $Revision: 14324 $

Info:

DCE/RPC and MSRPC Services Enumeration
Risk: Info
Application: msrpc
Port: 135
Protocol: tcp
ScriptID: 108044
Vulnerability Detection Result:
A DCE endpoint resolution service seems to be running on this port.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. The actual reporting takes place in the NVT 'DCE/RPC and MSRPC Services Enumeration Reporting' (OID: 1.3.6.1.4.1.25623.1.0.10736)
Solution:
Filter incoming traffic to this port.
Impact:
An attacker may use this fact to gain more knowledge about the remote host.
CVSS Base Score: 0.0
Family name: Windows
Category: infos
Copyright: This script is Copyright (C) 2001 Dave Aitel (ported to NASL by rd and Pavel Kankovsky)
Summary: NOSUMMARY
Version: $Revision: 11885 $

Info:

FileZilla Server Version Detection
Risk: Info
Application: ftp
Port: 21
Protocol: tcp
ScriptID: 900518
Vulnerability Detection Result:
Detected FileZilla Server
Version: 0.9.41
Location: 21/tcp
CPE: cpe:/a:filezilla:filezilla_server:0.9.41
Concluded from version/product identification result:
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
Detection of FileZilla Server
This script finds the version of FileZilla Server and sets the result in KB.
CVSS Base Score: 0.0
Family name: Product detection
Category: infos
Copyright: Copyright (C) 2009 SecPod
Summary: NOSUMMARY
Version: $Revision: 13499 $

Info:

FTP Banner Detection
Risk: Info
Application: ftp
Port: 21
Protocol: tcp
ScriptID: 10092
Vulnerability Detection Result:
Remote FTP server banner:
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
This is probably:
- FileZilla
Server operating system information collected via "SYST" command:
215 UNIX emulated by FileZilla
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
This Plugin detects and reports a FTP Server Banner.
CVSS Base Score: 0.0
Family name: Product detection
Category: infos
Copyright: This script is Copyright (C) 1999 SecuriTeam
Summary: NOSUMMARY
Version: 2019-06-24T08:34:07+0000

Info:

FTP Missing Support For AUTH TLS
Risk: Info
Application: ftp
Port: 21
Protocol: tcp
ScriptID: 108553
Vulnerability Detection Result:
The remote FTP server does not support the 'AUTH TLS' command.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
The remote FTP server does not support the 'AUTH TLS' command.
CVSS Base Score: 0.0
Family name: FTP
Category: unknown
Copyright: Copyright (C) 2019 Greenbone Networks GmbH
Version: $Revision: 13863 $

Info:

HTTP Security Headers Detection
Risk: Info
Application: https
Port: 443
Protocol: tcp
ScriptID: 112081
Vulnerability Detection Result:
Missing Headers

Content-Security-Policy
Referrer-Policy
X-Content-Type-Options
X-Frame-Options
X-Permitted-Cross-Domain-Policies
X-XSS-Protection
Summary:
All known security headers are being checked on the host. On completion a report will hand back whether a specific security header
has been implemented (including its value) or is missing on the target.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
References:
https://www.owasp.org/index.php/OWASP_Secure_Headers_Project
https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#tab=Headers
https://securityheaders.io/
CVSS Base Score: 0.0
Family name: General
Category: infos
Copyright: This script is Copyright (C) 2017 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 10899 $

Info:

HTTP Security Headers Detection
Risk: Info
Application: http
Port: 80
Protocol: tcp
ScriptID: 112081
Vulnerability Detection Result:
Missing Headers

Content-Security-Policy
Referrer-Policy
X-Content-Type-Options
X-Frame-Options
X-Permitted-Cross-Domain-Policies
X-XSS-Protection
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
All known security headers are being checked on the host. On completion a report will hand back whether a specific security header
has been implemented (including its value) or is missing on the target.
References:
https://www.owasp.org/index.php/OWASP_Secure_Headers_Project
https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#tab=Headers
https://securityheaders.io/
CVSS Base Score: 0.0
Family name: General
Category: infos

Summary: NOSUMMARY
Version: $Revision: 10899 $

Info:

HTTP Server type and version
Risk: Info
Application: https
Port: 443
Protocol: tcp
ScriptID: 10107
Vulnerability Detection Result:
The remote web server type is :
Apache/2.4.37 (Win32) OpenSSL/1.0.2p PHP/7.0.33
Solution : You can set the directive "ServerTokens Prod" to limit
the information emanating from the server in its response headers.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
This detects the HTTP Server's type and version.
Solution:
- Configure your server to use an alternate name like
'Wintendo httpD w/Dotmatrix display'
- Be sure to remove common logos like apache_pb.gif.
- With Apache, you can set the directive 'ServerTokens Prod' to limit
the information emanating from the server in its response headers.
CVSS Base Score: 0.0
Family name: Web Servers
Category: infos
Copyright: This script is Copyright (C) 2000 H. Scholz & Contributors
Summary: NOSUMMARY
Version: $Revision: 11585 $

Info:

HTTP Server type and version
Risk: Info
Application: http
Port: 80
Protocol: tcp
ScriptID: 10107
Vulnerability Detection Result:
The remote web server type is :
Apache/2.4.37 (Win32) OpenSSL/1.0.2p PHP/7.0.33
Solution : You can set the directive "ServerTokens Prod" to limit
the information emanating from the server in its response headers.
Solution:
- Configure your server to use an alternate name like
'Wintendo httpD w/Dotmatrix display'
- Be sure to remove common logos like apache_pb.gif.
- With Apache, you can set the directive 'ServerTokens Prod' to limit
the information emanating from the server in its response headers.
Summary:
This detects the HTTP Server's type and version.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Web Servers
Category: infos
Copyright: This script is Copyright (C) 2000 H. Scholz & Contributors
Summary: NOSUMMARY
Version: $Revision: 11585 $

Info:

IMAP Missing Support For STARTTLS
Risk: Info
Application: imap
Port: 143
Protocol: tcp
ScriptID: 108551
Vulnerability Detection Result:
The remote IMAP server does not support the 'STARTTLS' command.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
The remote IMAP server does not support the 'STARTTLS' command.
CVSS Base Score: 0.0
Family name: General
Category: unknown
Copyright: Copyright (C) 2019 Greenbone Networks GmbH
Version: $Revision: 13862 $

Info:

IMAP Banner
Risk: Info
Application: imap
Port: 143
Protocol: tcp
ScriptID: 11414
Vulnerability Detection Result:
Remote IMAP server banner:
* OK localhost IMAP4rev1 Mercury/32 v4.62 server ready.
The remote IMAP server is announcing the following available CAPABILITIES via an unencrypted connection:
AUTH=PLAIN, X-MERCURY-1
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
This detects the IMAP Server's type and version by connecting to
the server and processing the received banner.
CVSS Base Score: 0.0
Family name: General
Category: infos
Copyright: This script is Copyright (C) 2003 StrongHoldNet
Summary: NOSUMMARY
Version: $Revision: 13637 $

Info:

jQuery Detection
Risk: Info
Application: https
Port: 443
Protocol: tcp
ScriptID: 141622
Vulnerability Detection Result:
Detected jQuery
Version: 1.10.2
Location: //code.jquery.com
CPE: cpe:/a:jquery:jquery:1.10.2
Concluded from version/product identification result:
src="//code.jquery.com/jquery-1.10.2.min.js
Summary:
Detection of jQuery.
The script sends a connection request to the server and attempts to detect jQuery and to extract its version.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
References:
https://jquery.com/
CVSS Base Score: 0.0
Family name: Product detection
Category: infos
Copyright: Copyright (C) 2018 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 14001 $

Info:

jQuery Detection
Risk: Info
Application: http
Port: 80
Protocol: tcp
ScriptID: 141622
Vulnerability Detection Result:
Detected jQuery
Version: 1.10.2
Location: //code.jquery.com
CPE: cpe:/a:jquery:jquery:1.10.2
Concluded from version/product identification result:
src="//code.jquery.com/jquery-1.10.2.min.js
Summary:
Detection of jQuery.
The script sends a connection request to the server and attempts to detect jQuery and to extract its version.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
References:
https://jquery.com/
CVSS Base Score: 0.0
Family name: Product detection
Category: infos
Copyright: Copyright (C) 2018 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 14001 $

Info:

LDAP Detection
Risk: Info
Application: finger
Port: 79
Protocol: tcp
ScriptID: 100082
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
A LDAP Server is running at this host.
The Lightweight Directory Access Protocol, or LDAP is an application
protocol for querying and modifying directory services running over
TCP/IP.
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: This script is Copyright (C) 2009 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 13541 $

Info:

MySQL/MariaDB Detection
Risk: Info
Application: mysql
Port: 3306
Protocol: tcp
ScriptID: 100152
Vulnerability Detection Result:
Detected MariaDB
Version: unknown
Location: 3306/tcp
CPE: cpe:/a:mariadb:mariadb
Extra information:
Scanner received a ER_HOST_NOT_PRIVILEGED error from the remote MariaDB server.
Some tests may fail. Allow the scanner to access the remote MariaDB server for better results.
Summary:
Detects the installed version of
MySQL/MariaDB.
Detect a running MySQL/MariaDB by getting the banner, extract the version
from the banner and store the information in KB.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Product detection
Category: infos

Summary: NOSUMMARY
Version: $Revision: 10929 $

Info:

Nikto (NASL wrapper)
Risk: Info
Application: https
Port: 443
Protocol: tcp
ScriptID: 14260
Vulnerability Detection Result:
Here is the Nikto report:
Unknown option: useragent
-config+ Use this config file
-Display+ Turn on/off display outputs
-dbcheck check database and other key files for syntax errors
-Format+ save file (-o) format
-Help Extended help information
-host+ target host
-id+ Host authentication to use, format is id:pass or id:pass:realm
-list-plugins List all available plugins
-output+ Write output to this file
-nossl Disables using SSL
-no404 Disables 404 checks
-Plugins+ List of plugins to run (default: ALL)
-port+ Port to use (default 80)
-root+ Prepend root value to all requests, format is /directory
-ssl Force ssl mode on port
-Tuning+ Scan tuning
-timeout+ Timeout for requests (default 10 seconds)
-update Update databases and plugins from CIRT.net
-Version Print plugin and database versions
-vhost+ Virtual host (for Host header)
+ requires a value
Note: This is the short help output. Use -H for full help text.
Summary:
This plugin uses nikto to find weak CGI scripts and other known issues
regarding web server security. See the preferences section for configuration options.
Note: The plugin needs the 'nikto' or 'nikto.pl' binary found within the PATH of the user running the scanner and needs to be executable for this user. The existence of this binary is checked and reported separately within 'Availability of scanner helper tools' (OID: 1.3.6.1.4.1.25623.1.0.810000).
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Web application abuses
Category: infos
Copyright: This script is Copyright (C) 2004 Michel Arboi
Summary: NOSUMMARY
Version: $Revision: 13985 $

Info:

Nikto (NASL wrapper)
Risk: Info
Application: http
Port: 80
Protocol: tcp
ScriptID: 14260
Vulnerability Detection Result:
Here is the Nikto report:
Unknown option: useragent
-config+ Use this config file
-Display+ Turn on/off display outputs
-dbcheck check database and other key files for syntax errors
-Format+ save file (-o) format
-Help Extended help information
-host+ target host
-id+ Host authentication to use, format is id:pass or id:pass:realm
-list-plugins List all available plugins
-output+ Write output to this file
-nossl Disables using SSL
-no404 Disables 404 checks
-Plugins+ List of plugins to run (default: ALL)
-port+ Port to use (default 80)
-root+ Prepend root value to all requests, format is /directory
-ssl Force ssl mode on port
-Tuning+ Scan tuning
-timeout+ Timeout for requests (default 10 seconds)
-update Update databases and plugins from CIRT.net
-Version Print plugin and database versions
-vhost+ Virtual host (for Host header)
+ requires a value
Note: This is the short help output. Use -H for full help text.
Summary:
This plugin uses nikto to find weak CGI scripts and other known issues
regarding web server security. See the preferences section for configuration options.
Note: The plugin needs the 'nikto' or 'nikto.pl' binary found within the PATH of the user running the scanner and needs to be executable for this user. The existence of this binary is checked and reported separately within 'Availability of scanner helper tools' (OID: 1.3.6.1.4.1.25623.1.0.810000).
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Web application abuses
Category: infos
Copyright: This script is Copyright (C) 2004 Michel Arboi
Summary: NOSUMMARY
Version: $Revision: 13985 $

Info:

OpenSSL Remote Version Detection
Risk: Info
Application: https
Port: 443
Protocol: tcp
ScriptID: 806723
Vulnerability Detection Result:
Detected OpenSSL
Version: 1.0.2p
Location: 443/tcp
CPE: cpe:/a:openssl:openssl:1.0.2p
Concluded from version/product identification result:
OpenSSL/1.0.2p
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
Detects the installed version of
OpenSSL.
This script sends HTTP GET request and try to get the version from the
response, and sets the result in KB.
CVSS Base Score: 0.0
Family name: Product detection
Category: infos
Copyright: Copyright (C) 2015 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 13901 $

Info:

OS Detection Consolidation and Reporting
Risk: Info
Application: general
Port: 0
Protocol: tcp
ScriptID: 105937
Vulnerability Detection Result:
Best matching OS:
OS: Microsoft Windows
CPE: cpe:/o:microsoft:windows
Found by NVT: 1.3.6.1.4.1.25623.1.0.105355 (FTP OS Identification)
Concluded from FTP banner on port 21/tcp: 220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Setting key "Host/runs_windows" based on this information
Other OS detections (in order of reliability):
OS: Windows 7 Ultimate 7601 Service Pack 1
CPE: cpe:/o:microsoft:windows_7:-:sp1
Found by NVT: 1.3.6.1.4.1.25623.1.0.102011 (SMB NativeLanMan)
Concluded from SMB/Samba banner on port 445/tcp: OS String: Windows 7 Ultimate 7601 Service Pack 1; SMB String: Windows 7 Ultimate 6.1
OS: Microsoft Windows
CPE: cpe:/o:microsoft:windows
Found by NVT: 1.3.6.1.4.1.25623.1.0.111067 (HTTP OS Identification)
Concluded from HTTP Server banner on port 80/tcp: Server: Apache/2.4.37 (Win32) OpenSSL/1.0.2p PHP/7.0.33
OS: Microsoft Windows
CPE: cpe:/o:microsoft:windows
Found by NVT: 1.3.6.1.4.1.25623.1.0.111067 (HTTP OS Identification)
Concluded from HTTP Server banner on port 443/tcp: Server: Apache/2.4.37 (Win32) OpenSSL/1.0.2p PHP/7.0.33
OS: Microsoft Windows
CPE: cpe:/o:microsoft:windows
Found by NVT: 1.3.6.1.4.1.25623.1.0.108044 (DCE/RPC and MSRPC Services Enumeration)
Concluded from DCE/RPC and MSRPC Services Enumeration on port 135/tcp
Summary:
This script consolidates the OS information detected by several NVTs and tries to find the best matching OS.
Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional information
which might help to improve the OS detection.
If any of this information is wrong or could be improved please consider to report these to the referenced community portal.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
References:
https://community.greenbone.net/c/vulnerability-tests
CVSS Base Score: 0.0
Family name: Product detection
Category: infos
Copyright: This script is Copyright (C) 2016 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: 2019-06-01T08:20:43+0000

Info:

PHP Version Detection (Remote)
Risk: Info
Application: https
Port: 443
Protocol: tcp
ScriptID: 800109
Vulnerability Detection Result:
Detected PHP
Version: 7.0.33
Location: 443/tcp
CPE: cpe:/a:php:php:7.0.33
Concluded from version/product identification result:
Server: Apache/2.4.37 (Win32) OpenSSL/1.0.2p PHP/7.0.33
Summary:
Detects the installed version of PHP.
This script sends HTTP GET request and try to get the version from the response, and sets the result in KB.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Product detection
Category: infos

Summary: NOSUMMARY
Version: $Revision: 13811 $

Info:

PHP Version Detection (Remote)
Risk: Info
Application: http
Port: 80
Protocol: tcp
ScriptID: 800109
Vulnerability Detection Result:
Detected PHP
Version: 7.0.33
Location: 80/tcp
CPE: cpe:/a:php:php:7.0.33
Concluded from version/product identification result:
Server: Apache/2.4.37 (Win32) OpenSSL/1.0.2p PHP/7.0.33
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
Detects the installed version of PHP.
This script sends HTTP GET request and try to get the version from the response, and sets the result in KB.
CVSS Base Score: 0.0
Family name: Product detection
Category: infos
Copyright: Copyright (C) 2008 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 13811 $

Info:

Ping Host
Risk: Info
Application: general
Port: 0
Protocol: tcp
ScriptID: 100315
Vulnerability Detection Result:
The alive test was not launched because no method was selected.
Summary:
This check tries to determine whether a remote host is up (alive).
Several methods are used for this depending on configuration of this check. Whether a host is up can be detected in 3 different ways:
- A ICMP message is sent to the host and a response is taken as alive sign.
- An ARP request is sent and a response is taken as alive sign.
- A number of typical TCP services (namely the 20 top ports of nmap) are tried and their presence is taken as alive sign.
None of the methods is failsafe. It depends on network and/or host configurations whether they succeed or not. Both, false positives and false negatives can occur.
Therefore the methods are configurable.
If you select to not mark unreachable hosts as dead, no alive detections are executed and the host is assumed to be available for scanning.
In case it is configured that hosts are never marked as dead, this can cause considerable timeouts and therefore a long scan duration in case the hosts are in fact not available.
The available methods might fail for the following reasons:
- ICMP: This might be disabled for a environment and would then cause false negatives as hosts are believed to be dead that actually are alive. In contrast it is also possible that a Firewall between the scanner and the target host is answering to the ICMP message and thus hosts are believed to be alive that actually are dead.
- TCP ping: Similar to the ICMP case a Firewall between the scanner and the target might answer to the sent probes and thus hosts are believed to be alive that actually are dead.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Port scanners
Category: scanner

Summary: NOSUMMARY
Version: 2019-05-24T11:20:30+0000

Info:

POP3 Missing Support For STLS
Risk: Info
Application: pop-3
Port: 110
Protocol: tcp
ScriptID: 108552
Vulnerability Detection Result:
The remote POP3 server does not support the 'STLS' command.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
The remote POP3 server does not support the 'STLS' command.
CVSS Base Score: 0.0
Family name: General
Category: unknown

Version: $Revision: 13862 $

Info:

POP3 Server type and version
Risk: Info
Application: pop-3
Port: 110
Protocol: tcp
ScriptID: 10185
Vulnerability Detection Result:
Remote POP3 server banner:
+OK <52210945.30029@localhost>, POP3 server ready.
The remote POP3 server is announcing the following available CAPABILITIES via an unencrypted connection:
EXPIRE NEVER, TOP, UIDL, USER
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
This detects the POP3 Server's type and version by connecting to
the server and processing the received banner.
CVSS Base Score: 0.0
Family name: General
Category: infos

Summary: NOSUMMARY
Version: $Revision: 13836 $

Info:

Service Detection (3 ASCII digit codes like FTP, SMTP, NNTP...)
Risk: Info
Application: pop3pw
Port: 106
Protocol: tcp
ScriptID: 14773
Vulnerability Detection Result:
Although this service answers with 3 digit ASCII codes like FTP, SMTP or NNTP servers, the Scanner was unable to identify it.
This is highly suspicious and might be a backdoor; in this case, your system is compromised and an attacker can control it remotely.
** If you know what it is, consider this message as a false alert and please report it to the referenced community portal.
Solution : disinfect or reinstall your operating system.
Summary:
This plugin performs service detection.
This plugin is a complement of find_service.nasl. It attempts to
identify services that return 3 ASCII digit codes (ie: FTP, SMTP, NNTP, ...)
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
References:
https://community.greenbone.net/c/vulnerability-tests
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: This script is Copyright (C) 2004 Michel Arboi
Summary: NOSUMMARY
Version: $Revision: 13541 $

Info:

Services
Risk: Info
Application: finger
Port: 79
Protocol: tcp
ScriptID: 10330
Vulnerability Detection Result:
An unknown service is running on this port.
It is usually reserved for Finger
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
This routine attempts to guess which service is running on the
remote ports. For instance, it searches for a web server which could listen on another port than
80 or 443 and makes this information available for other check routines.
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>
Summary: NOSUMMARY
Version: $Revision: 13541 $

Info:

Services
Risk: Info
Application: ftp
Port: 21
Protocol: tcp
ScriptID: 10330
Vulnerability Detection Result:
An FTP server is running on this port.
Summary:
This routine attempts to guess which service is running on the
remote ports. For instance, it searches for a web server which could listen on another port than
80 or 443 and makes this information available for other check routines.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>
Summary: NOSUMMARY
Version: $Revision: 13541 $

Info:

Services
Risk: Info
Application: smtp
Port: 25
Protocol: tcp
ScriptID: 10330
Vulnerability Detection Result:
An SMTP server is running on this port
Here is its banner :
220 localhost ESMTP server ready.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
This routine attempts to guess which service is running on the
remote ports. For instance, it searches for a web server which could listen on another port than
80 or 443 and makes this information available for other check routines.
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>
Summary: NOSUMMARY
Version: $Revision: 13541 $

Info:

Services
Risk: Info
Application: http
Port: 80
Protocol: tcp
ScriptID: 10330
Vulnerability Detection Result:
A web server is running on this port
Summary:
This routine attempts to guess which service is running on the
remote ports. For instance, it searches for a web server which could listen on another port than
80 or 443 and makes this information available for other check routines.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>
Summary: NOSUMMARY
Version: $Revision: 13541 $

Info:

Services
Risk: Info
Application: pop-3
Port: 110
Protocol: tcp
ScriptID: 10330
Vulnerability Detection Result:
A pop3 server is running on this port
Summary:
This routine attempts to guess which service is running on the
remote ports. For instance, it searches for a web server which could listen on another port than
80 or 443 and makes this information available for other check routines.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>
Summary: NOSUMMARY
Version: $Revision: 13541 $

Info:

Services
Risk: Info
Application: mysql
Port: 3306
Protocol: tcp
ScriptID: 10330
Vulnerability Detection Result:
A MySQL server is running on this port
Summary:
This routine attempts to guess which service is running on the
remote ports. For instance, it searches for a web server which could listen on another port than
80 or 443 and makes this information available for other check routines.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>
Summary: NOSUMMARY
Version: $Revision: 13541 $

Info:

Services
Risk: Info
Application: https
Port: 443
Protocol: tcp
ScriptID: 10330
Vulnerability Detection Result:
A TLScustom server answered on this port
Summary:
This routine attempts to guess which service is running on the
remote ports. For instance, it searches for a web server which could listen on another port than
80 or 443 and makes this information available for other check routines.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>
Summary: NOSUMMARY
Version: $Revision: 13541 $

Info:

Services
Risk: Info
Application: https
Port: 443
Protocol: tcp
ScriptID: 10330
Vulnerability Detection Result:
A web server is running on this port through SSL
Summary:
This routine attempts to guess which service is running on the
remote ports. For instance, it searches for a web server which could listen on another port than
80 or 443 and makes this information available for other check routines.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>
Summary: NOSUMMARY
Version: $Revision: 13541 $

Info:

Services
Risk: Info
Application: imap
Port: 143
Protocol: tcp
ScriptID: 10330
Vulnerability Detection Result:
An IMAP server is running on this port
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
This routine attempts to guess which service is running on the
remote ports. For instance, it searches for a web server which could listen on another port than
80 or 443 and makes this information available for other check routines.
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>
Summary: NOSUMMARY
Version: $Revision: 13541 $

Info:

Services
Risk: Info
Application: csnet-ns
Port: 105
Protocol: tcp
ScriptID: 10330
Vulnerability Detection Result:
A PH server seems to be running on this port
Summary:
This routine attempts to guess which service is running on the
remote ports. For instance, it searches for a web server which could listen on another port than
80 or 443 and makes this information available for other check routines.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>
Summary: NOSUMMARY
Version: $Revision: 13541 $

Info:

Services
Risk: Info
Application: ssh
Port: 22
Protocol: tcp
ScriptID: 10330
Vulnerability Detection Result:
An ssh server is running on this port
Summary:
This routine attempts to guess which service is running on the
remote ports. For instance, it searches for a web server which could listen on another port than
80 or 443 and makes this information available for other check routines.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>
Summary: NOSUMMARY
Version: $Revision: 13541 $

Info:

SMB NativeLanMan
Risk: Info
Application: microsoft-ds
Port: 445
Protocol: tcp
ScriptID: 102011
Vulnerability Detection Result:
Detected SMB workgroup: WORKGROUP
Detected SMB server: Windows 7 Ultimate 6.1
Detected OS: Windows 7 Ultimate 7601 Service Pack 1
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
It is possible to extract OS, domain and SMB server information
from the Session Setup AndX Response packet which is generated during NTLM authentication.
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: Copyright (C) 2009 LSS
Summary: NOSUMMARY
Version: 2019-04-24T11:06:32+0000

172.20.1.132	Host-172-20-1-132

Info:

SSH Protocol Algorithms Supported
Risk: Info
Application: ssh
Port: 22
Protocol: tcp
ScriptID: 105565
Vulnerability Detection Result:
The following options are supported by the remote ssh service:
kex_algorithms:
curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256
server_host_key_algorithms:
rsa-sha2-512,rsa-sha2-256,ssh-rsa,ecdsa-sha2-nistp256,ssh-ed25519
encryption_algorithms_client_to_server:
chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com
encryption_algorithms_server_to_client:
chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com
mac_algorithms_client_to_server:
umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1
mac_algorithms_server_to_client:
umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1
compression_algorithms_client_to_server:
none,zlib@openssh.com
compression_algorithms_server_to_client:
none,zlib@openssh.com
Summary:
This script detects which algorithms and languages are supported by the remote SSH Service
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Service detection
Category: infos

Summary: NOSUMMARY
Version: $Revision: 13581 $

Info:

SSH Protocol Versions Supported
Risk: Info
Application: ssh
Port: 22
Protocol: tcp
ScriptID: 100259
Vulnerability Detection Result:
The remote SSH Server supports the following SSH Protocol Versions:
1.99
2.0
SSHv2 Fingerprint(s):
ecdsa-sha2-nistp256: 5b:18:19:bb:7b:6c:f3:06:f2:64:68:d3:9a:f1:73:20
ssh-rsa: 37:e8:96:95:f3:b6:17:d9:2f:56:c1:dd:21:2c:06:c0
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
Identification of SSH protocol versions supported by the remote
SSH Server. Also reads the corresponding fingerprints from the service.
The following versions are tried: 1.33, 1.5, 1.99 and 2.0
CVSS Base Score: 0.0
Family name: Service detection
Category: infos

Summary: NOSUMMARY
Version: $Revision: 13594 $

Info:

SSH Server type and version
Risk: Info
Application: ssh
Port: 22
Protocol: tcp
ScriptID: 10267
Vulnerability Detection Result:
Remote SSH server banner: SSH-2.0-OpenSSH_8.3
Remote SSH supported authentication: password,publickey,keyboard-interactive
Remote SSH text/login banner: (not available)
This is probably:
- OpenSSH
Concluded from remote connection attempt with credentials:
Login: OpenVAS-VT
Password: OpenVAS-VT
Summary:
This detects the SSH Server's type and version by connecting to the server
and processing the buffer received.
This information gives potential attackers additional information about the system they are attacking.
Versions and Types should be omitted where possible.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Product detection
Category: infos

Summary: NOSUMMARY
Version: 2019-06-05T03:32:14+0000

Info:

Traceroute
Risk: Info
Application: general
Port: 0
Protocol: tcp
ScriptID: 51662
Vulnerability Detection Result:
Here is the route from 172.20.1.127 to 172.20.1.132:
172.20.1.127
?
Solution:
Block unwanted packets from escaping your network.
Summary:
A traceroute from the scanning server to the target system was
conducted. This traceroute is provided primarily for informational value only. In the vast
majority of cases, it does not represent a vulnerability. However, if the displayed traceroute
contains any private addresses that should not have been publicly visible, then you have an
issue you need to correct.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: General
Category: infos

Summary: NOSUMMARY
Version: $Revision: 10411 $

Info:

Unknown OS and Service Banner Reporting
Risk: Info
Application: general
Port: 0
Protocol: tcp
ScriptID: 108441
Vulnerability Detection Result:
Unknown banners have been collected which might help to identify the OS running on this host. If these banners containing information about the host OS please report the following information to https://community.greenbone.net/c/vulnerability-tests:
Banner: # Nmap 7.30 scan initiated Sat Jan 25 03:21:41 2020 as: nmap -T3 -n -Pn -sV -oN /tmp/nmap-172.20.1.132-1153588589 -O --osscan-limit -p 22,21,25,80,135,139,443,445,12468,26702,37153 172.20.1.132
Nmap scan report for 172.20.1.132
Host is up (0.0048s latency).
PORT STATE SERVICE VERSION
21/tcp closed ftp
22/tcp open ssh OpenSSH 8.3 (protocol 2.0)
25/tcp closed smtp
80/tcp closed http
135/tcp closed msrpc
139/tcp closed netbios-ssn
443/tcp closed https
445/tcp closed microsoft-ds
12468/tcp closed unknown
26702/tcp closed unknown
37153/tcp closed unknown
MAC Address: 00:0C:29:28:12:F4 (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.30%E=4%D=1/25%OT=22%CT=21%CU=33997%PV=Y%DS=1%DC=D%G=Y%M=000C29%
OS:TM=5E2BB451%P=x86_64-unknown-linux-gnu)SEQ(SP=FF%GCD=1%ISR=103%TI=Z%CI=Z
OS:%II=I%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11
OS:NW7%O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE
OS:88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=4
OS:0%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O
OS:=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40
OS:%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q
OS:=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y
OS:%DFI=N%T=40%CD=S)
Network Distance: 1 hop
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done at Sat Jan 25 03:21:53 2020 -- 1 IP address (1 host up) scanned in 13.49 seconds
Identified from: Nmap TCP/IP fingerprinting
Summary:
This NVT consolidates and reports the information collected by
the following NVTs:
- Collect banner of unknown services (OID: 1.3.6.1.4.1.25623.1.0.11154)
- Service Detection (unknown) with nmap (OID: 1.3.6.1.4.1.25623.1.0.66286)
- Service Detection (wrapped) with nmap (OID: 1.3.6.1.4.1.25623.1.0.108525)
- OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)

If you know any of the information reported here, please send the full output to the referenced community portal.

CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
References:
https://community.greenbone.net/c/vulnerability-tests
CVSS Base Score: 0.0
Family name: Service detection
Category: infos

Summary: NOSUMMARY
Version: $Revision: 12934 $

Info:

CPE Inventory
Risk: Info
Application: general
Port: 0
Protocol: CPE-T
ScriptID: 810002
Vulnerability Detection Result:
172.20.1.132|cpe:/a:openbsd:openssh:8.3
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
This routine uses information collected by other routines about
CPE identities of operating systems, services and
applications detected during the scan.
References:
http://cpe.mitre.org/
CVSS Base Score: 0.0
Family name: Service detection
Category: end
Copyright: Copyright (c) 2009 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 14324 $

Info:

OpenSSH Detection Consolidation
Risk: Info
Application: general
Port: 0
Protocol: tcp
ScriptID: 108577
Vulnerability Detection Result:
Detected OpenSSH Server
Version: 8.3
Location: 22/tcp
CPE: cpe:/a:openbsd:openssh:8.3
Concluded from version/product identification result:
SSH-2.0-OpenSSH_8.3
Summary:
The script reports a detected OpenSSH including the
version number.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
References:
https://www.openssh.com/
CVSS Base Score: 0.0
Family name: Product detection
Category: unknown
Copyright: Copyright (C) 2019 Greenbone Networks GmbH
Version: 2019-05-23T06:42:35+0000

Info:

OS Detection Consolidation and Reporting
Risk: Info
Application: general
Port: 0
Protocol: tcp
ScriptID: 105937
Vulnerability Detection Result:
No Best matching OS identified. Please see the NVT 'Unknown OS and Service Banner Reporting' (OID: 1.3.6.1.4.1.25623.1.0.108441) for possible ways to identify this OS.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
This script consolidates the OS information detected by several NVTs and tries to find the best matching OS.
Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional information
which might help to improve the OS detection.
If any of this information is wrong or could be improved please consider to report these to the referenced community portal.
References:
https://community.greenbone.net/c/vulnerability-tests
CVSS Base Score: 0.0
Family name: Product detection
Category: infos

Summary: NOSUMMARY
Version: 2019-06-01T08:20:43+0000

Info:

Ping Host
Risk: Info
Application: general
Port: 0
Protocol: tcp
ScriptID: 100315
Vulnerability Detection Result:
The alive test was not launched because no method was selected.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
This check tries to determine whether a remote host is up (alive).
Several methods are used for this depending on configuration of this check. Whether a host is up can be detected in 3 different ways:
- A ICMP message is sent to the host and a response is taken as alive sign.
- An ARP request is sent and a response is taken as alive sign.
- A number of typical TCP services (namely the 20 top ports of nmap) are tried and their presence is taken as alive sign.
None of the methods is failsafe. It depends on network and/or host configurations whether they succeed or not. Both, false positives and false negatives can occur.
Therefore the methods are configurable.
If you select to not mark unreachable hosts as dead, no alive detections are executed and the host is assumed to be available for scanning.
In case it is configured that hosts are never marked as dead, this can cause considerable timeouts and therefore a long scan duration in case the hosts are in fact not available.
The available methods might fail for the following reasons:
- ICMP: This might be disabled for a environment and would then cause false negatives as hosts are believed to be dead that actually are alive. In contrast it is also possible that a Firewall between the scanner and the target host is answering to the ICMP message and thus hosts are believed to be alive that actually are dead.
- TCP ping: Similar to the ICMP case a Firewall between the scanner and the target might answer to the sent probes and thus hosts are believed to be alive that actually are dead.
CVSS Base Score: 0.0
Family name: Port scanners
Category: scanner

Summary: NOSUMMARY
Version: 2019-05-24T11:20:30+0000

Info:

Services
Risk: Info
Application: ssh
Port: 22
Protocol: tcp
ScriptID: 10330
Vulnerability Detection Result:
An ssh server is running on this port
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
This routine attempts to guess which service is running on the
remote ports. For instance, it searches for a web server which could listen on another port than
80 or 443 and makes this information available for other check routines.
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>
Summary: NOSUMMARY
Version: $Revision: 13541 $