Scan on 10.10.136.162

Script Author: Martin Zhelev Version: 1.0

Table of Contents

Table of Figures

Tool	Command	Tool Description
Nmap	sudo nmap -v -A -oX 10.10.57.101/output/outputNmap.xml 10.10.57.101	A network scanning tool used to discover devices running on a network.
Dirbuster	dirb http://10.10.57.101 -o 10.10.57.101/output/outputDirb.txtdirb http://10.10.57.101 -u Help:Listen -o 10.10.57.101/output/outputDirbLogged.txt	Web content scanning tool used for identifying hidden pages and files on webservers.
Nikto	nikto -h 10.10.57.101 -output 10.10.57.101/output/outputNikto.xml	Web server scanner that scans websites for vulnerabilities.
Hydra	hydra -v -f -u -o 10.10.57.101/credentials/credentials.json -b json -L 10.10.57.101/wordlists/wordlistUsernames.txt -P 10.10.57.101/wordlists/wordlistPasswords.txt 10.10.57.101 http-post-form '/login.php:username=^USER^&password;=^PASS^⊂=Login:Invalid username or password.'	Brute-forcing tool utilised for brute forcing web logins.
OpenVAS	N/A	Scans machines for vulnerabilities. Unlike Nikto it is not limited to just webservers.

Table of tools

Tool	Command	Tool Description
Nmap	sudo nmap -v -A -oX 10.10.57.101/output/outputNmap.xml 10.10.57.101	A network scanning tool used to discover devices running on a network.
Dirbuster	dirb http://10.10.57.101 -o 10.10.57.101/output/outputDirb.txtdirb http://10.10.57.101 -u Help:Listen -o 10.10.57.101/output/outputDirbLogged.txt	Web content scanning tool used for identifying hidden pages and files on webservers.
Nikto	nikto -h 10.10.57.101 -output 10.10.57.101/output/outputNikto.xml	Web server scanner that scans websites for vulnerabilities.
Hydra	hydra -v -f -u -o 10.10.57.101/credentials/credentials.json -b json -L 10.10.57.101/wordlists/wordlistUsernames.txt -P 10.10.57.101/wordlists/wordlistPasswords.txt 10.10.57.101 http-post-form '/login.php:username=^USER^&password;=^PASS^⊂=Login:Invalid username or password.'	Brute-forcing tool utilised for brute forcing web logins.
OpenVAS	N/A	Scans machines for vulnerabilities. Unlike Nikto it is not limited to just webservers.

1. Nmap

1.1. Output

```
Scan Information:
==============================================================
Scan Arguments: nmap -v -A -oX 10.10.136.162/output/outputNmap.xml
10.10.136.162
Scan Start Time: Tue Apr 23 01:52:33 2024
Scan Version: 7.94SVN
==============================================================
Host Information:
Host Address: 10.10.136.162
==============================================================
Open Ports:
----------------------------------------------------------------------------------------------------
Port: 22
Protocol: tcp
Service Name: ssh
Service Product: OpenSSH
Service Version: 8.2p1 Ubuntu 4ubuntu0.11
CPE 2.2: cpe:/a:openbsd:openssh:8.2p1
CPE 2.3: cpe:2.3:a:openbsd:openssh:8.2p1
Scripts ran:
-> ssh-hostkey: 3072 34:c4:a0:5c:f5:67:95:6f:72:95:b2:c4:78:29:2d:54 (RSA) 256
ce:2f:d3:0f:bd:44:4e:59:9d:73:c7:91:ff:17:d5:b1 (ECDSA) 256
82:64:cf:2d:71:0e:f3:2e:63:ff:fd:3f:a5:9f:70:3e (ED25519)
----------------------------------------------------------------------------------------------------
Port: 80
Protocol: tcp
Service Name: http
Service Product: Apache httpd
Service Version: 2.4.41
CPE 2.2: cpe:/a:apache:http_server:2.4.41
CPE 2.3: cpe:2.3:a:apache:http_server:2.4.41
Scripts ran:
-> http-title: Rick is sup4r cool
-> http-methods: Supported Methods: HEAD GET POST OPTIONS
-> http-server-header: Apache/2.4.41 (Ubuntu)
----------------------------------------------------------------------------------------------------
==============================================================
```

1.2. Recommendations

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

2. Nikto

2.1. Output

```
Scan Information:
==================================================================
Target IP: 10.10.136.162
Target hostname: 10.10.136.162
Target port: 80
Scan start time: 2024-04-23 01:52:54
==================================================================
Items:
--------------------------------------------------------------------------------------------------
Method: GET
Description: /: The anti-clickjacking X-Frame-Options header is not present.
URI: /
Reference:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
--------------------------------------------------------------------------------------------------
Method: GET
Description: /: The X-Content-Type-Options header is not set. This could allow the
user agent to render the content of the site in a different fashion to the MIME type.
URI: /
Reference: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/mi
ssing-content-type-header/
--------------------------------------------------------------------------------------------------
Method: GET
Description: /: Server may leak inodes via ETags, header found with file /, inode:
426, size: 5818ccf125686, mtime: gzip.
URI: /
Reference: CVE-2003-1418
--------------------------------------------------------------------------------------------------
Method: HEAD
Description: Apache/2.4.41 appears to be outdated (current is at least
Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
URI: /
Reference: Reference not available
--------------------------------------------------------------------------------------------------
Method: OPTIONS
Description: OPTIONS: Allowed HTTP Methods: HEAD, GET, POST, OPTIONS .
URI: /
Reference: Reference not available
--------------------------------------------------------------------------------------------------
Method: GET
Description: /login.php: Cookie PHPSESSID created without the httponly flag.
URI: /login.php
Reference: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
--------------------------------------------------------------------------------------------------
Method: GET
Description: /login.php: Admin login page/section found.
URI: /login.php
Reference: Reference not available
--------------------------------------------------------------------------------------------------
==================================================================
```

2.2. Recommendations

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

3. Dirbuster

3.1. Output

```
-----------------
DIRB v2.22
By The Dark Raver
-----------------

OUTPUT_FILE: 10.10.136.162/output/outputDirb.txt
START_TIME: Tue Apr 23 01:57:48 2024
URL_BASE: http://10.10.136.162/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.136.162/ ----
==> DIRECTORY: http://10.10.136.162/assets/
+ http://10.10.136.162/index.html (CODE:200|SIZE:1062)
+ http://10.10.136.162/robots.txt (CODE:200|SIZE:17)
+ http://10.10.136.162/server-status (CODE:403|SIZE:278)

---- Entering directory: http://10.10.136.162/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Tue Apr 23 02:02:50 2024
DOWNLOADED: 4612 - FOUND: 3
```

3.2. Recommendations

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

4. Dirbuster Logged

4.1. Output

```
-----------------
DIRB v2.22
By The Dark Raver
-----------------

OUTPUT_FILE: 10.10.136.162/output/outputDirbLogged.txt
START_TIME: Tue Apr 23 02:05:22 2024
URL_BASE: http://10.10.136.162/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
AUTHORIZATION: R1ckRul3s:Wubbalubbadubdub

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.136.162/ ----
==> DIRECTORY: http://10.10.136.162/assets/
+ http://10.10.136.162/index.html (CODE:200|SIZE:1062)
+ http://10.10.136.162/robots.txt (CODE:200|SIZE:17)
+ http://10.10.136.162/server-status (CODE:403|SIZE:278)

---- Entering directory: http://10.10.136.162/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Tue Apr 23 02:07:58 2024
DOWNLOADED: 4612 - FOUND: 3
```

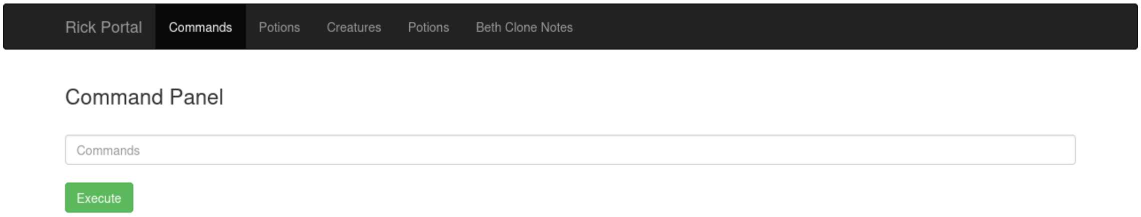
4.2. Recommendations

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

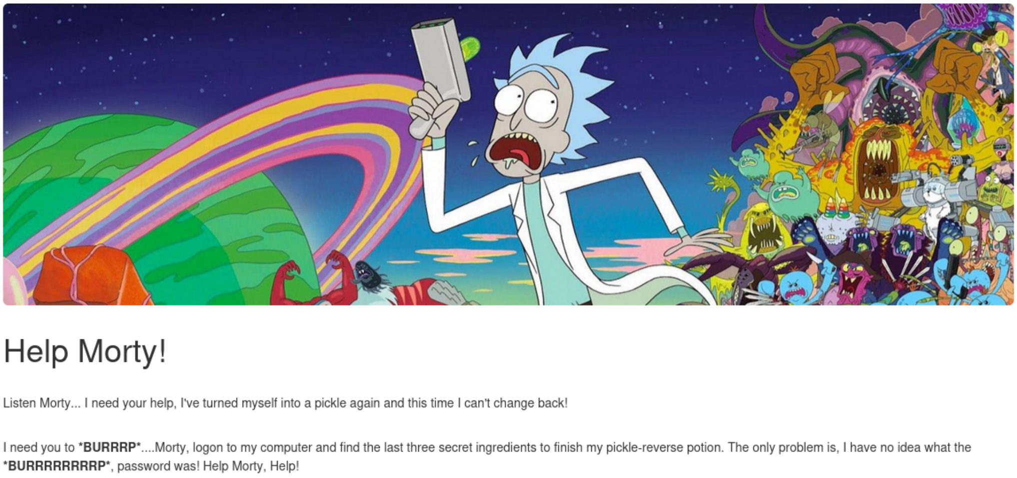
5. Screenshots

5.1. Output

5.1.1. 10.10.136.162.login.php.png



5.1.2. http...10.10.136.162.index.html.png

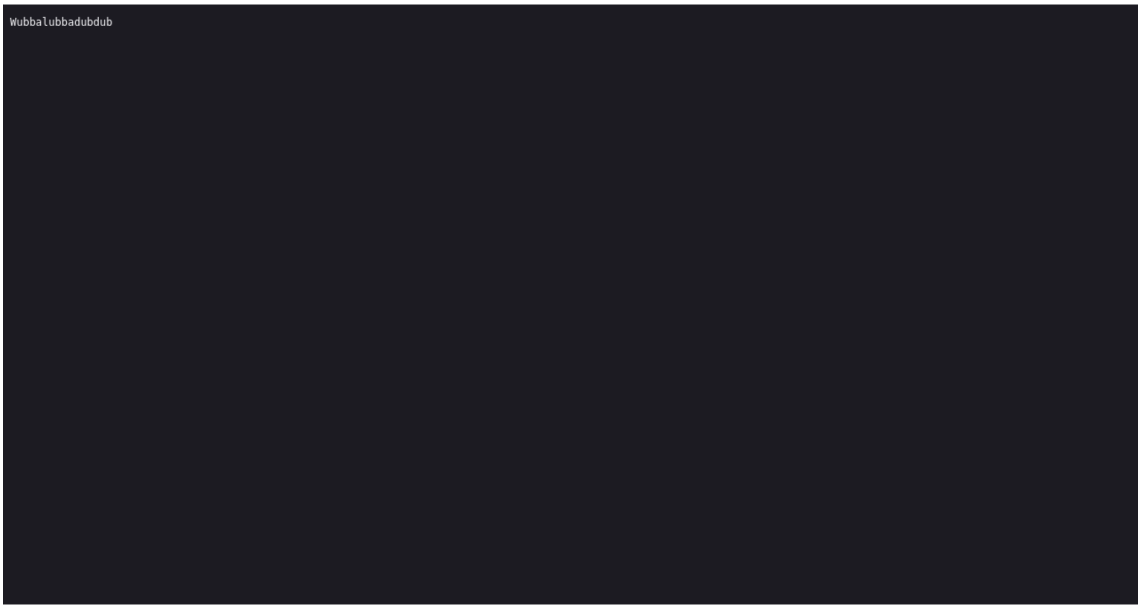


Help Morty!

Listen Morty... I need your help, I've turned myself into a pickle again and this time I can't change back!

I need you to ***BURRRP***....Morty, logon to my computer and find the last three secret ingredients to finish my pickle-reverse potion. The only problem is, I have no idea what the ***BURRRRRRRRP***, password was! Help Morty, Help!

5.1.3. http...10.10.136.162.robots.txt.png



```
Wubbalubbadubdub
```

6. Created Wordlists

6.1. Output

```
Note
to
self
remember
username
Username
R1ckRul3s
Rick
is
sup4r
cool
Help
Morty
Listen
Morty
I
need
your
help
Ive
turned
myself
into
a
pickle
again
and
this
time
I
cant
change
back
I
need
you
to
BURRRPMorty
logon
to
my
computer
and
find
the
last
three
secret
ingredients
to
finish
my
```

picklereverse
potion
The
only
problem
is
I
have
no
idea
what
the
BURRRRRRRRP
password
was
Help
Morty
Help
Wubbalubbadubdub

7. Discovered Credentails

7.1. Output

R1ckRul3s:Wubbalubbadubdub

8. Discovered CVEs

8.1. cpe:2.3:a:openbsd:openssh:8.2p1

8.1.1. CVE-2007-2768 (cpe:2.3:a:openbsd:openssh:8.2p1)

==

Title: cpe:2.3:a:openbsd:openssh:8.2p1
CVE ID: CVE-2007-2768
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2007-2768

Description: OpenSSH, when using OPIE (One-Time Passwords in Everything) for PAM, allows remote attackers to determine the existence of certain user accounts, which displays a different response if the user account exists and is configured to use one-time passwords (OTP), a similar issue to CVE-2007-2243.

Base Score: 4.3
Base Severity: None
Exploitablity Score: 8.6
Impract Score: 2.9

References:
http://archives.neohapsis.com/archives/fulldisclosure/2007-04/0635.html
http://www.osvdb.org/34601
https://security.netapp.com/advisory/ntap-20191107-0002/
http://secunia.com/advisories/31575
http://secunia.com/advisories/32241

==

8.1.2. CVE-2008-3844 (cpe:2.3:a:openbsd:openssh:8.2p1)

===

Title: cpe:2.3:a:openbsd:openssh:8.2p1
CVE ID: CVE-2008-3844
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2008-3844

Description: Certain Red Hat Enterprise Linux (RHEL) 4 and 5 packages for OpenSSH, as signed in August 2008 using a legitimate Red Hat GPG key, contain an externally introduced modification (Trojan Horse) that allows the package authors to have an unknown impact. NOTE: since the malicious packages were not distributed from any official Red Hat sources, the scope of this issue is restricted to users who may have obtained these packages through unofficial distribution points. As of 20080827, no unofficial distributions of this software are known.

Base Score: 9.3
Base Severity: None
Exploitablity Score: 8.6
Impract Score: 10.0

References:

http://archives.neohapsis.com/archives/fulldisclosure/2007-04/0635.html
http://www.osvdb.org/34601
https://security.netapp.com/advisory/ntap-20191107-0002/
http://secunia.com/advisories/31575
http://secunia.com/advisories/32241

===

8.1.3. CVE-2020-14145 (cpe:2.3:a:openbsd:openssh:8.2p1)

==

Title: cpe:2.3:a:openbsd:openssh:8.2p1
CVE ID: CVE-2020-14145
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2020-14145

Description: The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.

Base Score: 5.9
Base Severity: MEDIUM
Exploitablity Score: 2.2
Impract Score: 3.6

References:
http://archives.neohapsis.com/archives/fulldisclosure/2007-04/0635.html
http://www.osvdb.org/34601
https://security.netapp.com/advisory/ntap-20191107-0002/
http://secunia.com/advisories/31575
http://secunia.com/advisories/32241

==

8.1.4. CVE-2020-15778 (cpe:2.3:a:openbsd:openssh:8.2p1)

==

Title: cpe:2.3:a:openbsd:openssh:8.2p1
CVE ID: CVE-2020-15778
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2020-15778

Description: scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows."

Base Score: 7.8
Base Severity: HIGH
Exploitablity Score: 1.8
Impract Score: 5.9

References:
http://archives.neohapsis.com/archives/fulldisclosure/2007-04/0635.html
http://www.osvdb.org/34601
https://security.netapp.com/advisory/ntap-20191107-0002/
http://secunia.com/advisories/31575
http://secunia.com/advisories/32241

==

8.1.5. CVE-2021-28041 (cpe:2.3:a:openbsd:openssh:8.2p1)

==

Title: cpe:2.3:a:openbsd:openssh:8.2p1
CVE ID: CVE-2021-28041
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2021-28041

Description: ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.

Base Score: 7.1
Base Severity: HIGH
Exploitablity Score: 1.2
Impract Score: 5.9

References:
http://archives.neohapsis.com/archives/fulldisclosure/2007-04/0635.html
http://www.osvdb.org/34601
https://security.netapp.com/advisory/ntap-20191107-0002/
http://secunia.com/advisories/31575
http://secunia.com/advisories/32241

==

8.1.6. CVE-2016-20012 (cpe:2.3:a:openbsd:openssh:8.2p1)

===

Title: cpe:2.3:a:openbsd:openssh:8.2p1
CVE ID: CVE-2016-20012
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2016-20012

Description: OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product

----

Base Score: 5.3
Base Severity: MEDIUM
Exploitablity Score: 3.9
Impract Score: 1.4

References:
http://archives.neohapsis.com/archives/fulldisclosure/2007-04/0635.html
http://www.osvdb.org/34601
https://security.netapp.com/advisory/ntap-20191107-0002/
http://secunia.com/advisories/31575
http://secunia.com/advisories/32241

===

8.1.7. CVE-2021-41617 (cpe:2.3:a:openbsd:openssh:8.2p1)

==

Title: cpe:2.3:a:openbsd:openssh:8.2p1
CVE ID: CVE-2021-41617
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2021-41617

Description: sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

Base Score: 7.0
Base Severity: HIGH
Exploitablity Score: 1.0
Impract Score: 5.9

References:
http://archives.neohapsis.com/archives/fulldisclosure/2007-04/0635.html
http://www.osvdb.org/34601
https://security.netapp.com/advisory/ntap-20191107-0002/
http://secunia.com/advisories/31575
http://secunia.com/advisories/32241

==

8.1.8. CVE-2021-36368 (cpe:2.3:a:openbsd:openssh:8.2p1)

==

Title: cpe:2.3:a:openbsd:openssh:8.2p1
CVE ID: CVE-2021-36368
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2021-36368

Description: An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is "this is not an authentication bypass, since nothing is being bypassed.

Base Score: 3.7
Base Severity: LOW
Exploitablity Score: 2.2
Impract Score: 1.4

References:

http://archives.neohapsis.com/archives/fulldisclosure/2007-04/0635.html
http://www.osvdb.org/34601
https://security.netapp.com/advisory/ntap-20191107-0002/
http://secunia.com/advisories/31575
http://secunia.com/advisories/32241

==

8.1.9. CVE-2023-38408 (cpe:2.3:a:openbsd:openssh:8.2p1)

===

Title: cpe:2.3:a:openbsd:openssh:8.2p1
CVE ID: CVE-2023-38408
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2023-38408

Description: The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in /usr/lib is not necessarily safe for loading into ssh-agent.) NOTE: this issue exists because of an incomplete fix for CVE-2016-10009.

Base Score: 9.8
Base Severity: CRITICAL
Exploitablity Score: 3.9
Impract Score: 5.9

References:
http://archives.neohapsis.com/archives/fulldisclosure/2007-04/0635.html
http://www.osvdb.org/34601
https://security.netapp.com/advisory/ntap-20191107-0002/
http://secunia.com/advisories/31575
http://secunia.com/advisories/32241

===

8.1.10. CVE-2023-48795 (cpe:2.3:a:openbsd:openssh:8.2p1)

==

Title: cpe:2.3:a:openbsd:openssh:8.2p1
CVE ID: CVE-2023-48795
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2023-48795

Description: The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust.

Base Score: 5.9
Base Severity: MEDIUM
Exploitablity Score: 2.2
Impract Score: 3.6

References:

http://archives.neohapsis.com/archives/fulldisclosure/2007-04/0635.html
http://www.osvdb.org/34601
https://security.netapp.com/advisory/ntap-20191107-0002/
http://secunia.com/advisories/31575
http://secunia.com/advisories/32241

==

8.1.11. CVE-2023-51384 (cpe:2.3:a:openbsd:openssh:8.2p1)

==

Title: cpe:2.3:a:openbsd:openssh:8.2p1
CVE ID: CVE-2023-51384
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2023-51384

Description: In ssh-agent in OpenSSH before 9.6, certain destination constraints can be incompletely applied. When destination constraints are specified during addition of PKCS#11-hosted private keys, these constraints are only applied to the first key, even if a PKCS#11 token returns multiple keys.

Base Score: 5.5
Base Severity: MEDIUM
Exploitablity Score: 1.8
Impract Score: 3.6

References:
http://archives.neohapsis.com/archives/fulldisclosure/2007-04/0635.html
http://www.osvdb.org/34601
https://security.netapp.com/advisory/ntap-20191107-0002/
http://secunia.com/advisories/31575
http://secunia.com/advisories/32241

==

8.1.12. CVE-2023-51385 (cpe:2.3:a:openbsd:openssh:8.2p1)

===

Title: cpe:2.3:a:openbsd:openssh:8.2p1
CVE ID: CVE-2023-51385
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2023-51385

Description: In ssh in OpenSSH before 9.6, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.

Base Score: 6.5
Base Severity: MEDIUM
Exploitablity Score: 3.9
Impract Score: 2.5

References:
http://archives.neohapsis.com/archives/fulldisclosure/2007-04/0635.html
http://www.osvdb.org/34601
https://security.netapp.com/advisory/ntap-20191107-0002/
http://secunia.com/advisories/31575
http://secunia.com/advisories/32241

===

8.1.13. CVE-2023-51767 (cpe:2.3:a:openbsd:openssh:8.2p1)

===

Title: cpe:2.3:a:openbsd:openssh:8.2p1
CVE ID: CVE-2023-51767
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2023-51767

Description: OpenSSH through 9.6, when common types of DRAM are used, might allow row hammer attacks (for authentication bypass) because the integer value of authenticated in mm_answer_authpassword does not resist flips of a single bit. NOTE: this is applicable to a certain threat model of attacker-victim co-location in which the attacker has user privileges.

Base Score: 7.0
Base Severity: HIGH
Exploitablity Score: 1.0
Impract Score: 5.9

References:

http://archives.neohapsis.com/archives/fulldisclosure/2007-04/0635.html
http://www.osvdb.org/34601
https://security.netapp.com/advisory/ntap-20191107-0002/
http://secunia.com/advisories/31575
http://secunia.com/advisories/32241

===

8.2. cpe:2.3:a:apache:http_server:2.4.41

8.2.1. CVE-2007-4723 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41

CVE ID: CVE-2007-4723

CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2007-4723

Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

Base Score: 7.5

Base Severity: None

Exploitablity Score: 10.0

Impract Score: 6.4

References:

http://osvdb.org/45879

http://securityreason.com/securityalert/3100

http://www.securityfocus.com/archive/1/478263/100/0/threaded

http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html

http://secunia.com/advisories/34597

==

8.2.2. CVE-2009-0796 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2009-0796
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2009-0796

Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

Base Score: 2.6
Base Severity: None
Exploitablity Score: 4.9
Impract Score: 2.9

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.3. CVE-2009-2299 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2009-2299
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2009-2299

Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

Base Score: 5.0
Base Severity: None
Exploitablity Score: 10.0
Impract Score: 2.9

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.4. CVE-2011-1176 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2011-1176
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2011-1176

Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

Base Score: 4.3
Base Severity: None
Exploitablity Score: 8.6
Impract Score: 2.9

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.5. CVE-2011-2688 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2011-2688
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2011-2688

Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

Base Score: 7.5
Base Severity: None
Exploitablity Score: 10.0
Impract Score: 6.4

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.6. CVE-2012-3526 (cpe:2.3:a:apache:http_server:2.4.41)

===

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2012-3526
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2012-3526

Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

Base Score: 5.0
Base Severity: None
Exploitablity Score: 10.0
Impract Score: 2.9

References:

http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

===

8.2.7. CVE-2012-4001 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2012-4001
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2012-4001

Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

Base Score: 5.0
Base Severity: None
Exploitablity Score: 10.0
Impract Score: 2.9

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.8. CVE-2012-4360 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2012-4360
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2012-4360

Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

Base Score: 4.3
Base Severity: None
Exploitablity Score: 8.6
Impract Score: 2.9

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.9. CVE-2013-0941 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2013-0941
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2013-0941

Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

Base Score: 2.1
Base Severity: None
Exploitablity Score: 3.9
Impract Score: 2.9

References:

http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.10. CVE-2013-0942 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2013-0942
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2013-0942

Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

Base Score: 4.3
Base Severity: None
Exploitablity Score: 8.6
Impract Score: 2.9

References:

http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.11. CVE-2013-2765 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2013-2765
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2013-2765

Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

Base Score: 5.0
Base Severity: None
Exploitablity Score: 10.0
Impract Score: 2.9

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.12. CVE-2013-4365 (cpe:2.3:a:apache:http_server:2.4.41)

===

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2013-4365
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2013-4365

Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

Base Score: 7.5
Base Severity: None
Exploitablity Score: 10.0
Impract Score: 6.4

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

===

8.2.13. CVE-2020-1934 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2020-1934
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2020-1934

Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

Base Score: 5.3
Base Severity: MEDIUM
Exploitablity Score: 3.9
Impract Score: 1.4

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.14. CVE-2020-1927 (cpe:2.3:a:apache:http_server:2.4.41)

===

Title: cpe:2.3:a:apache:http_server:2.4.41

CVE ID: CVE-2020-1927

CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2020-1927

Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.

Base Score: 6.1

Base Severity: MEDIUM

Exploitablity Score: 2.8

Impract Score: 2.7

References:

http://osvdb.org/45879

http://securityreason.com/securityalert/3100

http://www.securityfocus.com/archive/1/478263/100/0/threaded

http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html

http://secunia.com/advisories/34597

===

8.2.15. CVE-2020-11984 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2020-11984
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2020-11984

Description: Apache HTTP server 2.4.32 to 2.4.44 mod_proxy_uwsgi info disclosure and possible RCE

Base Score: 9.8
Base Severity: CRITICAL
Exploitablity Score: 3.9
Impract Score: 5.9

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.16. CVE-2020-11993 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2020-11993
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2020-11993

Description: Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools. Configuring the LogLevel of mod_http2 above "info" will mitigate this vulnerability for unpatched servers.

Base Score: 7.5
Base Severity: HIGH
Exploitablity Score: 3.9
Impract Score: 3.6

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.17. CVE-2020-9490 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2020-9490
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2020-9490

Description: Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers.

Base Score: 7.5
Base Severity: HIGH
Exploitablity Score: 3.9
Impract Score: 3.6

References:

http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.18. CVE-2019-17567 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2019-17567
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2019-17567

Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

Base Score: 5.3
Base Severity: MEDIUM
Exploitablity Score: 3.9
Impract Score: 1.4

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.19. CVE-2020-13938 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2020-13938
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2020-13938

Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows

----

Base Score: 5.5
Base Severity: MEDIUM
Exploitablity Score: 1.8
Impract Score: 3.6

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.20. CVE-2020-13950 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2020-13950
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2020-13950

Description: Apache HTTP Server versions 2.4.41 to 2.4.46 mod_proxy_http can be made to crash (NULL pointer dereference) with specially crafted requests using both Content-Length and Transfer-Encoding headers, leading to a Denial of Service

----

Base Score: 7.5
Base Severity: HIGH
Exploitablity Score: 3.9
Impract Score: 3.6

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.21. CVE-2020-35452 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2020-35452
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2020-35452

Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

----

Base Score: 7.3
Base Severity: HIGH
Exploitablity Score: 3.9
Impract Score: 3.4

References:

http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.22. CVE-2021-26690 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2021-26690
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2021-26690

Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service

----

Base Score: 7.5
Base Severity: HIGH
Exploitablity Score: 3.9
Impract Score: 3.6

References:

http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.23. CVE-2021-26691 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2021-26691
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2021-26691

Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow

----

Base Score: 9.8
Base Severity: CRITICAL
Exploitablity Score: 3.9
Impract Score: 5.9

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.24. CVE-2021-30641 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2021-30641
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2021-30641

Description: Apache HTTP Server versions 2.4.39 to 2.4.46 Unexpected matching behavior with 'MergeSlashes OFF'

Base Score: 5.3
Base Severity: MEDIUM
Exploitablity Score: 3.9
Impract Score: 1.4

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.25. CVE-2021-32785 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41

CVE ID: CVE-2021-32785

CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2021-32785

Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache (`OIDCCacheEncrypt off`, `OIDCSessionType server-cache`, `OIDCCacheType redis`), `mod_auth_openidc` wrongly performed argument interpolation before passing Redis requests to `hiredis`, which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the `hiredis` API. As a workaround, this vulnerability can be mitigated by setting `OIDCCacheEncrypt` to `on`, as cache keys are cryptographically hashed before use when this option is enabled.

Base Score: 7.5

Base Severity: HIGH

Exploitablity Score: 3.9

Impract Score: 3.6

References:

http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.26. CVE-2021-32786 (cpe:2.3:a:apache:http_server:2.4.41)

===

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2021-32786
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2021-32786

Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, `oidc_validate_redirect_url()` does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring `mod_auth_openidc` to only allow redirection whose destination matches a given regular expression.

Base Score: 6.1
Base Severity: MEDIUM
Exploitablity Score: 2.8
Impract Score: 2.7

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

===

8.2.27. CVE-2021-32791 (cpe:2.3:a:apache:http_server:2.4.41)

===

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2021-32791
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2021-32791

Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.

Base Score: 5.9
Base Severity: MEDIUM
Exploitablity Score: 2.2
Impract Score: 3.6

References:

http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

===

8.2.28. CVE-2021-32792 (cpe:2.3:a:apache:http_server:2.4.41)

===

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2021-32792
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2021-32792

Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using `OIDCPreservePost On`.

Base Score: 6.1
Base Severity: MEDIUM
Exploitablity Score: 2.8
Impract Score: 2.7

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

===

8.2.29. CVE-2021-33193 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2021-33193
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2021-33193

Description: A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.

Base Score: 7.5
Base Severity: HIGH
Exploitablity Score: 3.9
Impract Score: 3.6

References:

http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.30. CVE-2021-34798 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2021-34798
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2021-34798

Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

Base Score: 7.5
Base Severity: HIGH
Exploitablity Score: 3.9
Impract Score: 3.6

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.31. CVE-2021-36160 (cpe:2.3:a:apache:http_server:2.4.41)

===

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2021-36160
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2021-36160

Description: A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS). This issue affects Apache HTTP Server versions 2.4.30 to 2.4.48 (inclusive).

Base Score: 7.5
Base Severity: HIGH
Exploitablity Score: 3.9
Impract Score: 3.6

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

===

8.2.32. CVE-2021-39275 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2021-39275
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2021-39275

Description: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

Base Score: 9.8
Base Severity: CRITICAL
Exploitablity Score: 3.9
Impract Score: 5.9

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.33. CVE-2021-40438 (cpe:2.3:a:apache:http_server:2.4.41)

===

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2021-40438
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2021-40438

Description: A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

Base Score: 9.0
Base Severity: CRITICAL
Exploitablity Score: 2.2
Impract Score: 6.0

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

===

8.2.34. CVE-2021-44224 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2021-44224
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2021-44224

Description: A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). This issue affects Apache HTTP Server 2.4.7 up to 2.4.51 (included).

Base Score: 8.2
Base Severity: HIGH
Exploitablity Score: 3.9
Impract Score: 4.2

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.35. CVE-2021-44790 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2021-44790
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2021-44790

Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

Base Score: 9.8
Base Severity: CRITICAL
Exploitablity Score: 3.9
Impract Score: 5.9

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.36. CVE-2022-22719 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2022-22719
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2022-22719

Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

Base Score: 7.5
Base Severity: HIGH
Exploitablity Score: 3.9
Impract Score: 3.6

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.37. CVE-2022-22720 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2022-22720
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2022-22720

Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

----

Base Score: 9.8
Base Severity: CRITICAL
Exploitablity Score: 3.9
Impract Score: 5.9

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.38. CVE-2022-22721 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2022-22721
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2022-22721

Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

Base Score: 9.1
Base Severity: CRITICAL
Exploitablity Score: 3.9
Impract Score: 5.2

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.39. CVE-2022-23943 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2022-23943
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2022-23943

Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

Base Score: 9.8
Base Severity: CRITICAL
Exploitablity Score: 3.9
Impract Score: 5.9

References:

http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.40. CVE-2022-26377 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2022-26377
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2022-26377

Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

Base Score: 7.5
Base Severity: HIGH
Exploitablity Score: 3.9
Impract Score: 3.6

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.41. CVE-2022-28330 (cpe:2.3:a:apache:http_server:2.4.41)

===

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2022-28330
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2022-28330

Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

Base Score: 5.3
Base Severity: MEDIUM
Exploitablity Score: 3.9
Impract Score: 1.4

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

===

8.2.42. CVE-2022-28614 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2022-28614
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2022-28614

Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

Base Score: 5.3
Base Severity: MEDIUM
Exploitablity Score: 3.9
Impract Score: 1.4

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.43. CVE-2022-28615 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2022-28615
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2022-28615

Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

Base Score: 9.1
Base Severity: CRITICAL
Exploitablity Score: 3.9
Impract Score: 5.2

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.44. CVE-2022-29404 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2022-29404
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2022-29404

Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

Base Score: 7.5
Base Severity: HIGH
Exploitablity Score: 3.9
Impract Score: 3.6

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.45. CVE-2022-30556 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2022-30556
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2022-30556

Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

Base Score: 7.5
Base Severity: HIGH
Exploitablity Score: 3.9
Impract Score: 3.6

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.46. CVE-2022-31813 (cpe:2.3:a:apache:http_server:2.4.41)

===

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2022-31813
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2022-31813

Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

Base Score: 9.8
Base Severity: CRITICAL
Exploitablity Score: 3.9
Impract Score: 5.9

References:

http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

===

8.2.47. CVE-2006-20001 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2006-20001
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2006-20001

Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash. This issue affects Apache HTTP Server 2.4.54 and earlier.

Base Score: 7.5
Base Severity: HIGH
Exploitablity Score: 3.9
Impract Score: 3.6

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.48. CVE-2022-36760 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2022-36760
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2022-36760

Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

Base Score: 9.0
Base Severity: CRITICAL
Exploitablity Score: 2.2
Impract Score: 6.0

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.49. CVE-2022-37436 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2022-37436
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2022-37436

Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

Base Score: 5.3
Base Severity: MEDIUM
Exploitablity Score: 3.9
Impract Score: 1.4

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.50. CVE-2023-25690 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2023-25690
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2023-25690

Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like: RewriteEngine on RewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P] ProxyPassReverse /here/ http://example.com:8080/ Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

Base Score: 9.8
Base Severity: CRITICAL
Exploitablity Score: 3.9
Impract Score: 5.9

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.51. CVE-2023-27522 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2023-27522
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2023-27522

Description: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55. Special characters in the origin response header can truncate/split the response forwarded to the client.

Base Score: 7.5
Base Severity: HIGH
Exploitablity Score: 3.9
Impract Score: 3.6

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.52. CVE-2023-31122 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2023-31122
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2023-31122

Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

Base Score: 7.5
Base Severity: HIGH
Exploitablity Score: 3.9
Impract Score: 3.6

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==

8.2.53. CVE-2023-45802 (cpe:2.3:a:apache:http_server:2.4.41)

==

Title: cpe:2.3:a:apache:http_server:2.4.41
CVE ID: CVE-2023-45802
CVE Link:https://nvd.nist.gov/vuln/detail/CVE-2023-45802

Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that. This was found by the reporter during testing of CVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out. Users are recommended to upgrade to version 2.4.58, which fixes the issue.

Base Score: 5.9
Base Severity: MEDIUM
Exploitablity Score: 2.2
Impract Score: 3.6

References:
http://osvdb.org/45879
http://securityreason.com/securityalert/3100
http://www.securityfocus.com/archive/1/478263/100/0/threaded
http://lists.apple.com/archives/security-announce/2010//Nov/msg00000.html
http://secunia.com/advisories/34597

==