Step 5: Final Report

Windows 10 ENT

Host	High	Medium	Low	Log
10.0.2.5	4	7	0	0

IP Address: 10.0.2.5

Service	Port	Sensitive Level
SMB / SMB2	135 139 445	High
HTTP	80 8080 80... TCP	Medium
MTS	3389 TCP	Low

Expected detail format for vulnerabilities found

- **Port 80**

High 7.5

1- CVE-2010-3964

Issue
Unrestricted file upload vulnerability in the Document Conversions Launcher Service in Microsoft Office SharePoint Server 2007 SP2, when the Document Conversions Load Balancer Service is enabled, allows remote attackers to execute arbitrary code via a crafted SOAP request to TCP port 8082, aka "Malformed Request Code Execution Vulnerability."

Impact
An attacker who successfully exploited this vulnerability could run arbitrary code in the security context of a guest user on the target server.

Mitigation
1. Stop and Disable Office Document Conversions Launcher Service
2. Block ports used by the Office Document Conversions Launcher Service at the firewall

Reference
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=2010-3964
- https://nvd.nist.gov/vuln/detail/CVE-2010-3964
- https://learn.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-104

Medium 4.3

2- CVE-2007-5277

Issue

Microsoft Internet Explorer 6 drops DNS pins based on failed connections to irrelevant TCP ports, which makes it easier for remote attackers to conduct DNS rebinding attacks, as demonstrated by a port 81 URL in an IMG SRC, when the DNS pin had been established for a session on port 80.

Impact

An attacker can exploit DNS rebinding vulnerabilities to circumvent firewalls and hijack IP addresses. The findings suggest that nearly 90% of web browsers are vulnerable.

Mitigation

1. Denying socket access
2. Check Host Header
3. Finer-grained Origins with IP address and public keys

Reference

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5277
- https://nvd.nist.gov/vuln/detail/CVE-2007-5277
- https://crypto.stanford.edu/dns/dns-rebinding.pdf

Medium 5.0

3- CVE-1999-0158

Issue

Cisco PIX firewall manager (PFM) on Windows NT allows attackers to connect to port 8080 on the PFM server and retrieve any file whose name and location is known.

Impact

If prerequisites are met, attackers can retrieve any file orfiles on the NT host on which PFM is installed, as well as any file or files on network servers accessible through that host's file system.

Mitigation

Use the PIX Device Manager instead of the PIX Firewall Manager (PFM). If that is not possible, upgrade to a version of PFM later than 4.2(1), or the latest version.

Reference

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5277
- https://nvd.nist.gov/vuln/detail/CVE-2007-5277
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-19980902-pix-mgr-file
- https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-19980902-pix-mgr-file.html

- **Port 135**

Medium 5.0

4- CVE-2006-3880

Issue
** DISPUTED ** Microsoft Windows NT 4.0, Windows 2000, Windows XP, and Windows Small Business Server 2003 allow remote attackers to cause a denial of service (IP stack hang) via a continuous stream of packets on TCP port 135 that have incorrect TCP header checksums and random numbers in certain TCP header fields, as demonstrated by the Achilles Windows Attack Tool.
NOTE: the researcher reports that the Microsoft Security Response Center has stated "Our investigation which has included code review, review of the TCPDump, and attempts on reproing the issue on multiple fresh installs of various Windows Operating Systems have all resulted in non confirmation."

Impact
Adversaries may perform Network Denial of Service (DoS) attacks to degrade or block the availability of targeted resources to users.

Mitigation
When flood volumes exceed the capacity of the network connection being targeted, it is typically necessary to intercept the incoming traffic upstream to filter out the attack traffic from the legitimate traffic.

Reference
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3880
- https://nvd.nist.gov/vuln/detail/CVE-2006-3880
- https://attack.mitre.org/techniques/T1498/

Medium 5.0

5- CVE-2002-1561

Issue
The RPC component in Windows 2000, Windows NT 4.0, and Windows XP allows remote attackers to cause a denial of service (disabled RPC service) via a malformed packet to the RPC Endpoint Mapper at TCP port 135, which triggers a null pointer dereference.

Impact
An unauthenticated, remote attacker could cause the RPC Endpoint Mapper to terminate, denying service to legitimate users. Since the RPC Endpoint Mapper is part of the RPC service, "...exploiting this vulnerability would cause the RPC service to fail, with the attendant loss of any RPC-based services the server offers, as well as potential loss of some COM functions."
Once the RPC service has been terminated, an attacker may be able to take control over an orphaned named pipe and gain the privileges of the RPC service (Local System).

Mitigation
Apply the appropriate patch (Q331953) as specified in MS03-010. Microsoft notes that a patch will not be produced for Windows NT 4.0 or Windows NT 4.0 Terminal Server Edition.
The patches may cause local COM calls to fail, which could affect ASP/COM+ applications. See Microsoft Knowledgebase Article 814119 for more information.

Reference
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3880
- https://www.kb.cert.org/vuls/id/261537
- https://learn.microsoft.com/en-us/security-updates/securitybulletins/2003/ms03-010

- **Port 139**

High 10.0

6- CVE-2007-5580

Issue
Buffer overflow in a certain driver in Cisco Security Agent 4.5.1 before 4.5.1.672, 5.0 before 5.0.0.225, 5.1 before 5.1.0.106, and 5.2 before 5.2.0.238 on Windows allows remote attackers to execute arbitrary code via a crafted SMB packet in a TCP session on port (1) 139 or (2) 445.

Impact
NSFOCUS Security Team discovered a remote buffer overflow vulnerability in Cisco Security Agent for Windows which allows remote code execution by sending a malicious SMB request.

Mitigation
Restrict access to TCP ports 139 and 445.

Reference
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5580
- https://nvd.nist.gov/vuln/detail/CVE-2007-5580
- https://cxsecurity.com/issue/WLB-2007120017

High 7.2

7- CVE-2004-1038

Issue
A design error in the IEEE1394 specification allows attackers with physical access to a device to read and write to sensitive memory using a modified FireWire/IEEE 1394 client, thus bypassing intended restrictions that would normally require greater degrees of physical access to exploit.
NOTE: this was reported in 2008 to affect Windows Vista, but some Linux-based operating systems have protection mechanisms against this attack.

Impact
The attack allows to have read and write access to computer memory. Windows password protection can be compromised.

Mitigation
Systems that require untrusted/unauthenticated physical access to require restricted operations, removal of wire headers connecting external case firewire jacks may provide some limited remediation. The primary precaution is not plug unknown/untrusted firewire devices into computers containing sensitive information. As this capability is built into the specification and chipsets at the hardware level, software fixes are still under investigation and will be discussed at the presentation.

Reference
- https://nvd.nist.gov/vuln/detail/CVE-2004-1038
- https://marc.info/?l=bugtraq&m=109881362530790&w=2
- https://www.theage.com.au/technology/hack-into-a-windows-pc-no-password-needed-20080305-gds3py.html

- **Port 445**

Medium 5.0

8- CVE-2002-0597

Issue
LANMAN service on Microsoft Windows 2000 allows remote attackers to cause a denial of service (CPU/ memory exhaustion) via a stream of malformed data to microsoft-ds port 445.

Impact
The complete impact of this vulnerability is not yet known. Consumption of memory will make applications fail in various ways and disrupt services provided by the system.

Mitigation
Upgrade to Windows 2000 Service Pack 3.

Reference

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0597
- https://nvd.nist.gov/vuln/detail/CVE-2002-0597
- https://www.kb.cert.org/vuls/id/693099

High 10.0

9- CVE-2007-5580

Issue
Buffer overflow in a certain driver in Cisco Security Agent 4.5.1 before 4.5.1.672, 5.0 before 5.0.0.225, 5.1 before 5.1.0.106, and 5.2 before 5.2.0.238 on Windows allows remote attackers to execute arbitrary code via a crafted SMB packet in a TCP session on port (1) 139 or (2) 445.

Impact
NSFOCUS Security Team discovered a remote buffer overflow vulnerability in Cisco Security Agent for Windows which allows remote code execution by sending a malicious SMB request.

Mitigation
Restrict access to TCP ports 139 and 445.

Reference

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5580
- https://nvd.nist.gov/vuln/detail/CVE-2007-5580
- https://cxsecurity.com/issue/WLB-2007120017

Medium 5.0

10- CVE-2002-0283

Issue

Windows XP with port 445 open allows remote attackers to cause a denial of service (CPU consumption) via a flood of TCP SYN packets containing possibly malformed data.

Impact

An Endpoint DoS denies the availability of a service without saturating the network used to provide access to the service. Adversaries target various layers of the application stack that is hosted on the system used to provide the service.

Mitigation

Leverage services provided by Content Delivery Networks (CDN) or providers specializing in DoS mitigations to filter traffic upstream from services. Filter boundary traffic by blocking source addresses sourcing the attack, blocking ports that are being targeted, or blocking protocols being used for transport. To defend against SYN floods, enable SYN Cookies.

Reference

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0283
- https://nvd.nist.gov/vuln/detail/CVE-2002-0283
- https://vuldb.com/?id.18214
- https://attack.mitre.org/techniques/T1499/
- https://exchange.xforce.ibmcloud.com/vulnerabilities/6912

- **Port 3389**

Medium 5.0

11- CVE-2001-0540

Issue
Memory leak in Terminal servers in Windows NT and Windows 2000 allows remote attackers to cause a denial of service (memory exhaustion) via a large number of malformed Remote Desktop Protocol (RDP) requests to port 3389.

Impact
If an attacker sent a sufficiently large quantity of such data to an affected machine, he could deplete the machine's memory to the point where response time would be slowed or the machine's ability to respond would be stopped altogether. All system services would be affected, including but not limited to terminal services.

Mitigation

- Apply the appropriate patch for your system, as listed in Microsoft Security Bulletin MS01-040, MS01-33, MS01-041, MS01-044 or MS02-018.

1. For Windows NT Server 4.0, Terminal Server Edition:
   Microsoft originally provided a patch for this vulnerability in MS01-040, but it has been superseded by the patch released with MS01-033, and then superseded by the patch released with MS02-018.
2. For Windows NT 4.0:
   Microsoft originally provided a patch for this vulnerability in MS01-033, MS01-041, and MS02-001, but they have been superseded by the Security Roll-up patch released with MS02-018.
3. For IIS:
   Microsoft originally provided a patch for this vulnerability in MS01-033, but it has been superseded by the patch released with MS01-044 and 02-018, and then superseded by the patch released with MS03-018.
4. For Windows 2000:
   Microsoft originally provided a patch for this vulnerability in MS01-033, but it has been superseded by the patch released with MS02-001.

Reference

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0540
- https://nvd.nist.gov/vuln/detail/CVE-2001-0540
- https://exchange.xforce.ibmcloud.com/vulnerabilities/6912

Ubuntu 18.04

Host	High	Medium	Low	Log
10.0.2.4	28	12	0	0

IP Address: 10.0.2.4

Service	Port	Sensitive Level
HTTP	80 TCP	High
SSL	22 TCP	Medium

- **Port 22**

Medium 5.9

1- CVE-2019-6111

Issue
An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).

Impact
Successful exploitation of these vulnerabilities could lead to disclosure of sensitive information or the addition or modification of data.

Mitigation
This issue only affects the users of scp binary which is a part of openssh-clients package. Other usage of SSH protocol or other ssh clients is not affected. Administrators can uninstall openssh-clients for additional protection against accidental usage of this binary. Removal or Update of openssh-clients package will make the packaged binaries like scp, ssh, etc, unavailable.

Reference
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6111
- https://nvd.nist.gov/vuln/detail/CVE-2019-6111
- https://access.redhat.com/security/cve/cve-2019-6111
- https://www.rapid7.com/db/vulnerabilities/openbsd-openssh-cve-2019-6111/
- https://security.netapp.com/advisory/ntap-20190213-0001/

Medium 5.3

2- CVE-2018-15919

Issue
Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.

Impact
Successful exploitation of this vulnerability could lead to disclosure of sensitive information.

Mitigation
If GSSAPI Authentication is not required, this flaw can be mitigated by changing the global configuration in `/etc/ssh/sshd_config` from `GSSAPIAuthentication yes` to `GSSAPIAuthentication no`.

Reference
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15919
- https://nvd.nist.gov/vuln/detail/CVE-2018-15919
- https://access.redhat.com/security/cve/cve-2018-15919
- https://security.netapp.com/advisory/ntap-20181221-0001/

Medium 5.3

3- CVE-2018-15473

Issue
OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.

Impact
Successful exploitation of this vulnerability could lead to disclosure of sensitive information.

Mitigation
Apply updates.

Reference
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15473
- https://nvd.nist.gov/vuln/detail/CVE-2018-15473
- https://security.netapp.com/advisory/ntap-20181101-0001/
- https://access.redhat.com/errata/RHSA-2019:2143
- https://access.redhat.com/articles/11258

- **Port 80**

High 7.5

4- CVE-2022-31813

Issue
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.

Impact
Successful exploitation of these vulnerabilities could lead to disclosure of sensitive information, addition or modification of data or Denial of Service (DoS).

Mitigation
Mitigation for this issue is either not available or the currently available options do not meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base or stability.

Reference
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31813
- https://nvd.nist.gov/vuln/detail/CVE-2022-31813
- https://access.redhat.com/security/cve/cve-2022-31813
- https://security.netapp.com/advisory/ntap-20220624-0005/

High 9.8 - **Critical**

5- CVE-2022-23943

Issue
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.

Impact
Successful exploitation of these vulnerabilities could lead to disclosure of sensitive information, addition or modification of data or Denial of Service (DoS).

Mitigation
Disabling mod_sed and restarting httpd will mitigate this flaw.

Reference
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23943
- https://nvd.nist.gov/vuln/detail/CVE-2022-23943
- https://access.redhat.com/security/cve/cve-2022-23943
- https://security.netapp.com/advisory/ntap-20220321-0001/

High 9.8 - Critical

6- CVE-2022-22720

Issue
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.

Impact
Successful exploitation of these vulnerabilities could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service (DoS).

Mitigation
There are currently no known mitigations for this issue.

Reference

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22720
- https://nvd.nist.gov/vuln/detail/cve-2022-22720
- https://security.netapp.com/advisory/ntap-20220321-0001/
- https://access.redhat.com/security/cve/cve-2022-22720

High 9.8 - Critical

7- CVE-2021-44790

Issue
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.

Impact
Successful exploitation of these vulnerabilities could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service (DoS).

Mitigation
Disabling mod_lua and restarting httpd will mitigate this flaw.

Reference

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44790
- https://nvd.nist.gov/vuln/detail/CVE-2021-44790
- https://access.redhat.com/security/cve/cve-2021-44790
- https://security.netapp.com/advisory/ntap-20211224-0001/

High 9.8 - Critical

8- CVE-2021-39275

Issue
Apache HTTP Server is vulnerable to a buffer overflow, caused by improper bounds checking by the ap_escape_quotes() function. By sending specially crafted input, a remote attacker could write beyond the end of a buffer.

Impact
Successful exploitation of these vulnerabilities could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service (DoS).

Mitigation
Mitigation for this issue is either not available or the currently available options do not meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base or stability.

Reference
- https://nvd.nist.gov/vuln/detail/cve-2021-39275
- https://access.redhat.com/security/cve/cve-2021-39275
- https://www.ibm.com/support/pages/security-bulletin-vulnerabilities-apache-http-cve-2021-34798-and-cve-2021-39275-affects-power-hmc
- https://security.netapp.com/advisory/ntap-20211008-0004/

High 9.8 - Critical

9- CVE-2021-26691

Issue
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.

Impact
Only configurations which use the "SessionEnv" directive (which is not widely used) are vulnerable to this flaw.

Mitigation
Upgrading to version 2.4.48 eliminates this vulnerability.

Reference
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26691
- https://nvd.nist.gov/vuln/detail/CVE-2021-26691
- https://access.redhat.com/security/cve/cve-2021-26691
- https://vuldb.com/?id.176768

High 7.8

10- CVE-2019-0211

Issue
In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.

Impact
Due to the elevated privileges obtained, there is an impact to the system beyond the web server itself.

Mitigation
CVE-2019-0211 is patched in Apache HTTP Server version 2.4.39. *Nix distributions including Ubuntu, Debian, and SuSE have package updates available for install. FreeBSD posted an advisory, but there is no security update available for it yet. Users are encouraged to install these updates as soon as possible.

Reference
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0211
- https://nvd.nist.gov/vuln/detail/CVE-2019-0211
- https://access.redhat.com/security/cve/cve-2019-0211
- https://www.tenable.com/blog/cve-2019-0211-proof-of-concept-for-apache-root-privilege-escalation-vulnerability-published

High 9.8 - **Critical**

11- CVE-2021-40438

Issue
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.

Impact
This vulnerability impacts Apache HTTP Server (aka httpd) version 2.4.48 and versions earlier than 2.4.48. Data from Shodan suggests that there are more than 500,000 servers matching this version, making it likely that attackers could find some fertile ground for leveraging this vulnerability in their attacks.

Mitigation
Update the server to version 2.4.51 and either disable the mod_proxy path or ensure it’s already disabled.

Reference
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40438
- https://nvd.nist.gov/vuln/detail/cve-2021-40438
- https://www.fastly.com/blog/apache-redux-preventing-server-side-request-forgery-via-cve-2021-40438

High 7.3

12- CVE-2020-35452

Issue
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.

Impact
The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

Mitigation
Only configurations which use mod_auth_digest are affected by this flaw. Also as per upstream this flaw is not exploitable in most conditions, so there should really be no impact of this flaw.

Reference

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-35452
- https://nvd.nist.gov/vuln/detail/CVE-2020-35452
- https://access.redhat.com/security/cve/cve-2020-35452

High 9.8 - **Critical**

13- CVE-2018-1312

Issue
In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

Impact
Authentication issues, an actor can claim an identity, the software does not prove or insufficiently proves that the claim is correct.

Mitigation
Upgrading to latest version eliminates this vulnerability.

Reference

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1312
- https://nvd.nist.gov/vuln/detail/CVE-2018-1312
- https://www.mend.io/vulnerability-database/CVE-2018-1312

High 8.1

14- CVE-2017-15715

Issue

In Apache httpd 2.4.0 to 2.4.29, the expression specified in <FilesMatch> could match '$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are are externally blocked, but only by matching the trailing portion of the filename.

Impact

The vulnerability was handled as a non-public zero-day exploit for at least 5 days. During that time the estimated underground price was around $25k-$100k.

Mitigation

Upgrading eliminates this vulnerability.

Reference

- https://nvd.nist.gov/vuln/detail/CVE-2017-15715
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15715
- https://vuldb.com/?id.115039
- https://www.mend.io/vulnerability-database/CVE-2017-15715

High 9.1 - Critical

15- CVE-2022-28615

Issue

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.

Impact

Very large input to the ap_strcmp_match function can lead to an integer overflow and result in an out-of-bounds read. Integer overflow or wraparound may lead to exposure of sensitive information to an unauthorized actor.

Mitigation

Upgrading to version 2.4.54 eliminates this vulnerability.

Reference

- https://nvd.nist.gov/vuln/detail/CVE-2022-28615
- https://support.f5.com/csp/article/K40582331
- https://vuldb.com/?id.201527

High 8.2

16- CVE-2021-44224

Issue
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).

Impact
It could cause a denial of service or compromise to confidentiality of data.

Mitigation
Upgrade to version 2.4.52 eliminates this vulnerability.

Reference
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44224
- https://nvd.nist.gov/vuln/detail/CVE-2021-44224
- https://httpd.apache.org/security/vulnerabilities_24.html

High 9.1 - **Critical**

17- CVE-2019-10082

Issue
In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown.

Impact
Referencing memory after it has been freed can cause a program to crash, use unexpected values, or execute code. This is going to have an impact on confidentiality, integrity, and availability.

Mitigation
There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

Reference
- https://nvd.nist.gov/vuln/detail/CVE-2019-10082
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10082
- https://vuldb.com/?id.142323

High 7.5

18- CVE-2019-0217

Issue
In Apache HTTP Server 2.4 release 2.4.38 and prior, 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.

Impact
The manipulation with an unknown input leads to a race condition vulnerability.

Mitigation
This flaw only affects a threaded server configuration, so using the prefork MPM is an effective mitigation.

Reference
- https://nvd.nist.gov/vuln/detail/CVE-2019-0217
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0217
- https://access.redhat.com/security/cve/cve-2019-0217
- https://vuldb.com/?id.133112

High 9.1 - Critical

19- CVE-2022-22721

Issue
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.

Impact
This issue can lead to an integer overflow and later causes an out-of-bounds write.

Mitigation
Set the LimitXMLRequestBody option to a value smaller than 350MB. Setting it to 0 is not recommended as it will use a hard limit (depending on 32bit or 64bit systems) which may result in an overall system out-of-memory. The default configuration is not vulnerable to this flaw, see the statement above.

Reference
- https://nvd.nist.gov/vuln/detail/CVE-2022-22721
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22721
- https://access.redhat.com/security/cve/cve-2022-22721

Medium 6.1

20- CVE-2020-1927

Issue
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.

Impact
This issue simplifies phishing attacks and later impact on confidentiality, integrity, and availability.

Mitigation
Upgrade to version 2.4.42 eliminates this vulnerability.

Reference
- https://nvd.nist.gov/vuln/detail/CVE-2020-1927
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1927
- https://vuldb.com/?id.152664
- https://httpd.apache.org/security/vulnerabilities_24.html

Medium 6.1

21- CVE-2019-10098

Issue
In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.

Impact
An attacker could abuse this flaw in a phishing attack or as part of a client-side attack on browsers.

Mitigation
This flaw requires the use of certain Rewrite configuration directives. The following command can be used to search for possible vulnerable configurations: grep -R '^\s*Rewrite' /etc/httpd/

Reference
- https://nvd.nist.gov/vuln/detail/CVE-2019-10098
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10098
- https://access.redhat.com/security/cve/cve-2019-10098
- https://httpd.apache.org/docs/2.4/mod/mod_rewrite.html

High 7.5

22- CVE-2022-30556

Issue
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.

Impact
Information disclosure.

Mitigation
Disabling mod_lua and restarting httpd will mitigate this flaw.

Reference
- https://nvd.nist.gov/vuln/detail/CVE-2022-30556
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30556
- https://access.redhat.com/security/cve/cve-2022-30556

High 7.5

23- CVE-2022-29404

Issue
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.

Impact
Lead to a denial of service due to no default limit on the possible input size.

Mitigation
Disabling mod_lua and restarting httpd will mitigate this flaw.

Reference
- https://nvd.nist.gov/vuln/detail/cve-2022-29404
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29404
- https://access.redhat.com/security/cve/cve-2022-29404

Medium 5.3

24- CVE-2022-28614

Issue
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.

Impact
Lead to an integer overflow which result in an out-of-bounds read and later impact on confidentiality.

Mitigation
Upgrading to version 2.4.54 eliminates this vulnerability.

Reference
- https://nvd.nist.gov/vuln/detail/CVE-2022-28614
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28614
- https://vuldb.com/?id.201531 (user/pass required)
- https://access.redhat.com/security/cve/cve-2022-28614

High 7.5

25- CVE-2022-26377

Issue
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.

Impact
This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions. This flaw allows an attacker to smuggle requests to the AJP server, where it forwards requests. Request smuggling vulnerabilities are often critical in nature, allowing an attacker to bypass security controls, gain unauthorized access to sensitive data, and directly compromise other application users.

Mitigation
Disabling mod_proxy_ajp and restarting httpd will mitigate this flaw.

Reference
- https://access.redhat.com/security/cve/cve-2022-26377
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26377
- https://nvd.nist.gov/vuln/detail/CVE-2022-26377
- https://cve.report/CVE-2022-26377
- https://portswigger.net/web-security/request-smuggling

High 7.5

26- CVE-2022-22719

Issue
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.

Impact
The highest threat from this vulnerability is to system availability.

Mitigation
Disabling mod_lua and restarting httpd will mitigate this flaw.

Reference
- https://nvd.nist.gov/vuln/detail/CVE-2022-22719
- https://access.redhat.com/security/cve/cve-2022-22719
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22719

High 7.5

27- CVE-2021-34798

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

Impact
The highest threat from this vulnerability is to system availability.

Mitigation
Restrict access to the affected systems, especially to port 443/tcp, to trusted IP addresses only.

Reference
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34798
- https://access.redhat.com/security/cve/cve-2021-34798
- https://cert-portal.siemens.com/productcert/pdf/ssa-685781.pdf
- https://github.com/advisories/GHSA-6cg7-x9gh-4wf6

High 7.5

28- CVE-2021-33193

Issue
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.

Impact
The highest threat from this flaw is to system integrity.

Mitigation
This flaw can be mitigated by disabling HTTP/2.

Reference
- https://nvd.nist.gov/vuln/detail/CVE-2021-33193
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33193
- https://access.redhat.com/security/cve/cve-2021-33193

High 7.5

29- CVE-2021-26690

Issue
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.

Impact
The highest threat from this vulnerability is to system availability.

Mitigation
Only configurations which use the "SessionEnv" directive (which is not widely used) are vulnerable to this flaw.

Reference
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26690
- https://nvd.nist.gov/vuln/detail/CVE-2021-26690
- https://access.redhat.com/security/cve/cve-2021-26690

High 7.5

30- CVE-2020-9490

Issue

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.

Impact

The highest threat from this vulnerability is to system availability.

Mitigation

Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability.

Reference

- https://nvd.nist.gov/vuln/detail/CVE-2020-9490
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9490
- https://access.redhat.com/security/cve/cve-2020-9490

Medium 5.3

31- CVE-2020-1934

Issue

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.

Impact

By sending a specially-crafted request, an attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service condition on the system.

Mitigation

Upgrade to the latest version of HTTP Server (2.4.42 or later), available from the Apache Web site.

Reference

- https://nvd.nist.gov/vuln/detail/CVE-2020-1934
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1934
- https://access.redhat.com/security/cve/cve-2020-1934
- https://vuldb.com/?id.152665
- https://www.ibm.com/support/pages/security-bulletin-vulnerabilities-cve-2020-1927-and-cve-2020-1934-apache-http-server-affect-ibm-i
- https://exchange.xforce.ibmcloud.com/vulnerabilities/178937

Medium 5.3

32- CVE-2019-17567

Issue

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.

Impact

When an actor claims to have a given identity, the software does not prove or insufficiently proves that the claim is correct. Impacted is confidentiality, integrity, and availability.

Mitigation

Only configurations which use mod_proxy_wstunnel are affected by this flaw. It is also safe to comment-out the "LoadModule proxy_wstunnel_module ... " line in /etc/httpd/conf.modules.d/00-proxy.conf for configurations which do not rely on a websockets reverse proxy.

Reference

- https://nvd.nist.gov/vuln/detail/CVE-2019-17567
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17567
- https://access.redhat.com/security/cve/cve-2019-17567
- https://vuldb.com/?id.176765

High 7.5

33- CVE-2019-10081

Issue

HTTP/2 (2.4.20 through 2.4.39) very early pushes, for example configured with "H2PushResource", could lead to an overwrite of memory in the pushing request's pool, leading to crashes. The memory copied is that of the configured push link header values, not data supplied by the client.

Impact

Under certain circumstances, HTTP/2 early pushes could lead to memory corruption, causing a server to crash.

Mitigation

This flaw is only exploitable if Apache httpd is configured to respond to HTTP/2 requests, which is done by including "h2" or "h2c" in the "Protocols" list in a configuration file. The following command can be used to search for possible vulnerable configurations: grep -R '^\s*Protocols\>.*\<h2\>' /etc/httpd/

Reference

- https://nvd.nist.gov/vuln/detail/CVE-2019-10081
- https://access.redhat.com/security/cve/CVE-2019-10081
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10081

Medium 5.3

34- CVE-2019-0220

Issue
A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. 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.

Impact
The manipulation as part of Regular Expression leads to denial of service, confidentiality, and availability.

Mitigation
This flaw can be mitigation by replacing multiple consecutive slashes, used in directives that match against the path component of the request URL with regular expressions.

Reference

- https://nvd.nist.gov/vuln/detail/CVE-2019-0220
- https://access.redhat.com/security/cve/cve-2019-0220
- https://vuldb.com/?id.136374
- https://cve.circl.lu/cve/CVE-2019-0220

Medium 5.3

35- CVE-2019-0196

Issue
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.

Impact
Referencing memory after it has been freed can cause a program to crash, use unexpected values, or execute code.

Mitigation
Upgrade to version 2.4.39 eliminates this vulnerability.

Reference

- https://nvd.nist.gov/vuln/detail/CVE-2019-0196
- https://vuldb.com/?id.136372
- https://access.redhat.com/security/cve/cve-2019-0196

High 7.5

36- CVE-2018-17199

Issue

In Apache HTTP Server 2.4 release 2.4.37 and prior, 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.

Impact

Authenticating a user, or otherwise establishing a new user session, without invalidating any existing session identifier gives an attacker the opportunity to steal authenticated sessions. As an impact it is known to affect confidentiality, integrity, and availability.

Mitigation

Upgrading eliminates this vulnerability.

Reference

- https://nvd.nist.gov/vuln/detail/CVE-2018-17199
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-17199
- https://vuldb.com/?id.130330

Medium 5.3

37- CVE-2018-17189

Issue

In Apache HTTP server versions 2.4.37 and prior, 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 (mod_http2) connections.

Impact

This is going to have an impact on availability. Adversaries may perform Endpoint Denial of Service (DoS) attacks to degrade or block the availability of services to users.

Mitigation

Upgrading eliminates this vulnerability.

Reference

- https://nvd.nist.gov/vuln/detail/CVE-2018-17189
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-17189
- https://vuldb.com/?id.130329
- https://attack.mitre.org/techniques/T1499/

High 7.5

38- CVE-2018-1333

Issue
By specially crafting HTTP/2 requests, workers would be allocated 60 seconds longer than necessary, leading to worker exhaustion and a denial of service. Fixed in Apache HTTP Server 2.4.34 (Affected 2.4.18-2.4.30,2.4.33).

Impact
The manipulation leads to denial of service, the exploitation appears to be easy.

Mitigation
Upgrading to version 2.4.34 eliminates this vulnerability.

Reference

- https://nvd.nist.gov/vuln/detail/CVE-2018-1333
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1333
- https://vuldb.com/?id.122569

High 7.5

39- CVE-2018-1303

Issue
A specially crafted HTTP request header could have crashed the Apache HTTP Server prior to version 2.4.30 due to an out of bound read while preparing data to be cached in shared memory.

Impact
The manipulation as part of a Request Header leads to a information disclosure vulnerability, also affect confidentiality, and availability.

Mitigation
Upgrading to version 2.4.30 eliminates this vulnerability.

Reference

- https://nvd.nist.gov/vuln/detail/CVE-2018-1303
- https://access.redhat.com/security/cve/cve-2018-1303
- https://vuldb.com/?id.115060

High 7.5

40- CVE-2017-15710

Issue

In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.

Impact

The manipulation leads to memory corruption and an impact on availability.

Mitigation

Upgrading eliminates this vulnerability.

Reference

- https://nvd.nist.gov/vuln/detail/CVE-2017-15710
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15710
- https://vuldb.com/?id.115038