Flan Scan Report

December 8, 2019

Summary

Team20 used Cloudflare's Flan Scan to assess the entire network.
Please see the end of the report for the closed ports
Flan Scan ran a network vulnerability scan with the following Nmap command on Sat Nov 23 20:36:49 2019UTC.

```
nmap -sV -oX <output-file> -oN - -v1 --script=vulners/vulners.nse
```

To find out what IPs were scanned see the end of this report.

Services with Vulnerabilities

1 Apache httpd 2.4.38 (cpe:/a:apache:http_server:2.4.38)

CVE-2019-0211 High (7.2)

Summary: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.

CVE-2019-10082 Medium (6.4)

Summary: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.

CVE-2019-10097 Medium (6.0)

Summary:In Apache HTTP Server 2.4.32-2.4.39, when mod_remoteip was configured to use a trusted intermediary proxy server using the "PROXY" protocol, a specially crafted PROXY header could trigger a stack buffer overflow or NULL pointer deference. This vulnerability could only be triggered by a trusted proxy and not by untrusted HTTP clients.

CVE-2019-0215 Medium (6.0)

Summary:In Apache HTTP Server 2.4 releases 2.4.37 and 2.4.38, a bug in mod_ssl when using per-location client certificate verification with TLSv1.3 allowed a client to bypass configured access control restrictions.

CVE-2019-10098 Medium (5.8)

Summary: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.

CVE-2019-10081 Medium (5.0)

Summary: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.

CVE-2019-0220 Medium (5.0)

Summary: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.

CVE-2019-0196 Medium (5.0)

Summary:A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. 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.

CVE-2019-0197 Medium (4.9)

Summary:A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38. When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. Server that never enabled the h2 protocol or that only enabled it for https: and did not set ”H2Upgrade on” are unaffected by this issue.

CVE-2019-10092 Medium (4.3)

Summary:In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.

The above 10 vulnerabilities apply to these network locations:

- 192.168.0.14 Ports: [’80’, ’8080’]
- 192.168.0.13 Ports: [’80’, ’443’]
- 192.168.0.16 Ports: [’80’]

2 OpenSSH 7.5 (cpe:/a:openbsd:openssh:7.5)

CVE-2018-15919 Medium (5.0)

Summary: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.’

CVE-2017-15906 Medium (5.0)

Summary:The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.

The above 2 vulnerabilities apply to these network locations:

- 192.168.0.11 Ports: [’22’]
- 10.100.120.2 Ports: [’22’]

3 Samba smbd 4.6.2 (cpe:/a:samba:samba:4.6.2)

CVE-2017-7494 High (10.0)

Summary:Samba since version 3.5.0 and before 4.6.4, 4.5.10 and 4.4.14 is vulnerable to remote code execution vulnerability, allowing a malicious client to upload a shared library to a writable share, and then cause the server to load and execute it.

CVE-2017-14746 High (7.5)

Summary:Use-after-free vulnerability in Samba 4.x before 4.7.3 allows remote attackers to execute arbitrary code via a crafted SMB1 request.

CVE-2017-11103 Medium (6.8)

Summary:Heimdal before 7.4 allows remote attackers to impersonate services with Orpheus’ Lyre attacks because it obtains service-principal names in a way that violates the Kerberos 5 protocol specification. In _krb5_extract_ticket() the KDC-REP service name must be obtained from the encrypted version stored in ’enc_part’ instead of the unencrypted version stored in ’ticket’. Use of the unencrypted version provides an opportunity for successful server impersonation and other attacks. NOTE: this CVE is only for Heimdal and other products that embed Heimdal code; it does not apply to other instances in which this part of the Kerberos 5 protocol specification is violated.

CVE-2018-10858 Medium (6.5)

Summary:A heap-buffer overflow was found in the way samba clients processed extra long filename in a directory listing. A malicious samba server could use this flaw to cause arbitrary code execution on a samba client. Samba versions before 4.6.16, 4.7.9 and 4.8.4 are vulnerable.

CVE-2018-1057 Medium (6.5)

Summary:On a Samba 4 AD DC the LDAP server in all versions of Samba from 4.0.0 onwards incorrectly validates permissions to modify passwords over LDAP allowing authenticated users to change any other users’ passwords, including administrative users and privileged service accounts (eg Domain Controllers).

CVE-2017-12151 Medium (5.8)

Summary:A flaw was found in the way samba client before samba 4.4.16, samba 4.5.14 and samba 4.6.8 used encryption with the max protocol set as SMB3. The connection could lose the requirement for signing and encrypting to any DFS redirects, allowing an attacker to read or alter the contents of the connection via a man-in-the-middle attack.

CVE-2017-12150 Medium (5.8)

Summary:It was found that samba before 4.4.16, 4.5.x before 4.5.14, and 4.6.x before 4.6.8 did not enforce ”SMB signing” when certain configuration options were enabled. A remote attacker could launch a man-in-the-middle attack and retrieve information in plain-text.

CVE-2019-3880 Medium (5.5)

Summary:A flaw was found in the way samba implemented an RPC endpoint emulating the Windows registry service API. An unprivileged attacker could use this flaw to create a new registry hive file anywhere they have unix permissions which could lead to creation of a new file in the Samba share. Versions before 4.8.11, 4.9.6 and 4.10.2 are vulnerable.

CVE-2017-15275 Medium (5.0)

Summary:Samba before 4.7.3 might allow remote attackers to obtain sensitive information by leveraging failure of the server to clear allocated heap memory.

CVE-2019-14833 Medium (4.9)

Summary:A flaw was found in Samba, all versions starting samba 4.5.0 before samba 4.9.15, samba 4.10.10, samba 4.11.2, in the way it handles a user password change or a new password for a samba user. The Samba Active Directory Domain Controller can be configured to use a custom script to check for password complexity. This configuration can fail to verify password complexity when non-ASCII characters are used in the password, which could lead to weak passwords being set for samba users, making it vulnerable to dictionary attacks.

CVE-2017-12163 Medium (4.8)

Summary:An information leak flaw was found in the way SMB1 protocol was implemented by Samba before 4.4.16, 4.5.x before 4.5.14, and 4.6.x before 4.6.8. A malicious client could use this flaw to dump server memory contents to a file on the samba share or to a shared printer, though the exact area of server memory cannot be controlled by the attacker.

CVE-2019-10218 Medium (4.3)

Summary:A flaw was found in the samba client, all samba versions before samba 4.11.2, 4.10.10 and 4.9.15, where a malicious server can supply a pathname to the client with separators. This could allow the client to access files and folders outside of the SMB network pathnames. An attacker could use this vulnerability to create files outside of the current working directory using the privileges of the client user.

CVE-2018-1139 Medium (4.3)

Summary:A flaw was found in the way samba before 4.7.9 and 4.8.4 allowed the use of weak NTLMv1 authentication even when NTLMv1 was explicitly disabled. A man-in-the-middle attacker could use this flaw to read the credential and other details passed between the samba server and client.

CVE-2019-3824 Medium (4.0)

Summary:A flaw was found in the way an LDAP search expression could crash the shared LDAP server process of a samba AD DC in samba before version 4.10. An authenticated user, having read permissions on the LDAP server, could use this flaw to cause denial of service.

CVE-2019-14847 Medium (4.0)

Summary:A flaw was found in samba 4.0.0 before samba 4.9.15 and samba 4.10.x before 4.10.10. An attacker can crash AD DC LDAP server via dirsync resulting in denial of service. Privilege escalation is not possible with this issue.

CVE-2018-16851 Medium (4.0)

Summary:Samba from version 4.0.0 and before versions 4.7.12, 4.8.7, 4.9.3 is vulnerable to a denial of service. During the processing of an LDAP search before Samba's AD DC returns the LDAP entries to the client, the entries are cached in a single memory object with a maximum size of 256MB. When this size is reached, the Samba process providing the LDAP service will follow the NULL pointer, terminating the process. There is no further vulnerability associated with this issue, merely a denial of service.

CVE-2018-16841 Medium (4.0)

Summary:Samba from version 4.3.0 and before versions 4.7.12, 4.8.7 and 4.9.3 are vulnerable to a denial of service. When configured to accept smart-card authentication, Samba's KDC will call talloc_free() twice on the same memory if the principal in a validly signed certificate does not match the principal in the AS-REQ. This is only possible after authentication with a trusted certificate. talloc is robust against further corruption from a double-free with talloc_free() and directly calls abort(), terminating the KDC process.

CVE-2018-14629 Medium (4.0)

Summary:A denial of service vulnerability was discovered in Samba's LDAP server before versions 4.7.12, 4.8.7, and 4.9.3. A CNAME loop could lead to infinite recursion in the server. An unprivileged local attacker could create such an entry, leading to denial of service.

CVE-2018-10919 Medium (4.0)

Summary:The Samba Active Directory LDAP server was vulnerable to an information disclosure flaw because of missing access control checks. An authenticated attacker could use this flaw to extract confidential attribute values using LDAP search expressions. Samba versions before 4.6.16, 4.7.9 and 4.8.4 are vulnerable.

CVE-2018-1050 Low (2.9)

Summary:All versions of Samba from 4.0.0 onwards are vulnerable to a denial of service attack when the RPC spoolss service is configured to be run as an external daemon. Missing input sanitization checks on some of the input parameters to spoolss RPC calls could cause the print spooler service to crash.

The above 20 vulnerabilities apply to these network locations:

- 192.168.0.11 Ports: [’139’, ’445’]

4 OpenSSH 7.4 (cpe:/a:openbsd:openssh:7.4)

CVE-2018-15919 Medium (5.0)

Summary: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.’

CVE-2017-15906 Medium (5.0)

Summary:The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.

The above 2 vulnerabilities apply to these network locations:

- 192.168.0.10 Ports: [’22’]
- 192.168.0.8 Ports: [’22’]

5 Apache httpd 2.4.7 (cpe:/a:apache:http_server:2.4.7)

CVE-2017-7679 High (7.5)

Summary:In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

CVE-2018-1312 Medium (6.8)

Summary: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.

CVE-2017-15715 Medium (6.8)

Summary: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.

CVE-2014-0226 Medium (6.8)

Summary:Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2017-9788 Medium (6.4)

Summary:In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.

CVE-2019-10098 Medium (5.8)

Summary: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.

CVE-2019-0220 Medium (5.0)

Summary: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.

CVE-2018-17199 Medium (5.0)

Summary: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.

CVE-2017-9798 Medium (5.0)

Summary:Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.

CVE-2017-15710 Medium (5.0)

Summary: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.

CVE-2016-8743 Medium (5.0)

Summary:Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2016-2161 Medium (5.0)

Summary:In Apache HTTP Server versions 2.4.0 to 2.4.23, malicious input to mod_auth_digest can cause the server to crash, and each instance continues to crash even for subsequently valid requests.

CVE-2016-0736 Medium (5.0)

Summary:In Apache HTTP Server versions 2.4.0 to 2.4.23, mod_session_crypto was encrypting its data/cookie using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default), hence no selectable or builtin authenticated encryption. This made it vulnerable to padding oracle attacks, particularly with CBC.

CVE-2014-3523 Medium (5.0)

Summary:Memory leak in the winnt_accept function in server/mpm/winnt/child.c in the WinNT MPM in the Apache HTTP Server 2.4.x before 2.4.10 on Windows, when the default AcceptFilter is enabled, allows remote attackers to cause a denial of service (memory consumption) via crafted requests.

CVE-2014-0231 Medium (5.0)

Summary:The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.

CVE-2019-10092 Medium (4.3)

Summary:In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.

CVE-2016-4975 Medium (4.3)

Summary:Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the ”Location” or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).

CVE-2015-3185 Medium (4.3)

Summary:The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2014-8109 Medium (4.3)

Summary:mod_lua.c in the mod_lua module in the Apache HTTP Server 2.3.x and 2.4.x through 2.4.10 does not support an httpd configuration in which the same Lua authorization provider is used with different arguments within different contexts, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Require directives, as demonstrated by a configuration that specifies authorization for one group to access a certain directory, and authorization for a second group to access a second directory.

CVE-2014-0118 Medium (4.3)

Summary:The deflate_in_filter function in mod_deflate.c in the mod_deflate module in the Apache HTTP Server before 2.4.10, when request body decompression is enabled, allows remote attackers to cause a denial of service (resource consumption) via crafted request data that decompresses to a much larger size.

CVE-2014-0117 Medium (4.3)

Summary:The mod_proxy module in the Apache HTTP Server 2.4.x before 2.4.10, when a reverse proxy is enabled, allows remote attackers to cause a denial of service (child-process crash) via a crafted HTTP Connection header.

CVE-2018-1283 Low (3.5)

Summary:In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to forward its session data to CGI applications (SessionEnv on, not the default), a remote user may influence their content by using a ”Session” header. This comes from the ”HTTP_SESSION” variable name used by mod_session to forward its data to CGIs, since the prefix ”HTTP_” is also used by the Apache HTTP Server to pass HTTP header fields, per CGI specifications.

CVE-2016-8612 Low (3.3)

Summary:Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process.

The above 23 vulnerabilities apply to these network locations:

- 192.168.0.12 Ports: [’80’]

6 OpenSSH 7.2 (cpe:/a:openbsd:openssh:7.2)

CVE-2016-8858 High (7.8)

Summary:** DISPUTED ** The kex_input_kexinit function in kex.c in OpenSSH 6.x and 7.x through 7.3 allows remote attackers to cause a denial of service (memory consumption) by sending many duplicate KEXINIT requests. NOTE: a third party reports that ”OpenSSH upstream does not consider this as a security issue.”

CVE-2018-15919 Medium (5.0)

Summary: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.’

CVE-2017-15906 Medium (5.0)

Summary:The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.

CVE-2016-10708 Medium (5.0)

Summary:sshd in OpenSSH before 7.4 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence NEWKEYS message, as demonstrated by Honggfuzz, related to kex.c and packet.c.

The above 4 vulnerabilities apply to these network locations:

- 192.168.0.15 Ports: [’22’]

7 Apache httpd 2.4.20 (cpe:/a:apache:http_server:2.4.20)

CVE-2017-7679 High (7.5)

Summary:In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

CVE-2017-7668 High (7.5)

Summary:The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allows ap_find_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap_find_token() to return an incorrect value.

CVE-2017-3169 High (7.5)

Summary:In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.

CVE-2017-3167 High (7.5)

Summary:In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.

CVE-2019-0211 High (7.2)

Summary: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.

CVE-2018-1312 Medium (6.8)

Summary: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.

CVE-2017-15715 Medium (6.8)

Summary: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.

CVE-2019-10082 Medium (6.4)

Summary: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.

CVE-2017-9788 Medium (6.4)

Summary:In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type ’Digest’ was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no ’=’ assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.

CVE-2019-10098 Medium (5.8)

Summary: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.

CVE-2019-10081 Medium (5.0)

Summary: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.

CVE-2019-0220 Medium (5.0)

Summary: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.

CVE-2019-0196 Medium (5.0)

Summary:A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. 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.

CVE-2018-17199 Medium (5.0)

Summary: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.

CVE-2018-1333 Medium (5.0)

Summary: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).

CVE-2017-9798 Medium (5.0)

Summary:Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user’s .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.

CVE-2017-15710 Medium (5.0)

Summary: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.

CVE-2016-8743 Medium (5.0)

Summary:Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2016-8740 Medium (5.0)

Summary:The mod_http2 module in the Apache HTTP Server 2.4.17 through 2.4.23, when the Protocols configuration includes h2 or h2c, does not restrict request-header length, which allows remote attackers to cause a denial of service (memory consumption) via crafted CONTINUATION frames in an HTTP/2 request.

CVE-2016-4979 Medium (5.0)

Summary:The Apache HTTP Server 2.4.18 through 2.4.20, when mod_http2 and mod_ssl are enabled, does not properly recognize the ”SSLVerifyClient require” directive for HTTP/2 request authorization, which allows remote attackers to bypass intended access restrictions by leveraging the ability to send multiple requests over a single connection and aborting a renegotiation.

CVE-2016-2161 Medium (5.0)

Summary:In Apache HTTP Server versions 2.4.0 to 2.4.23, malicious input to mod_auth_digest can cause the server to crash, and each instance continues to crash even for subsequently valid requests.

CVE-2016-0736 Medium (5.0)

Summary:In Apache HTTP Server versions 2.4.0 to 2.4.23, mod_session_crypto was encrypting its data/cookie using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default), hence no selectable or builtin authenticated encryption. This made it vulnerable to padding oracle attacks, particularly with CBC.

CVE-2019-0197 Medium (4.9)

Summary:A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38. When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. Server that never enabled the h2 protocol or that only enabled it for https: and did not set ”H2Upgrade on” are unaffected by this issue.

CVE-2019-10092 Medium (4.3)

Summary:In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.

CVE-2018-11763 Medium (4.3)

Summary:In Apache HTTP Server 2.4.17 to 2.4.34, by sending continuous, large SETTINGS frames a client can occupy a connection, server thread and CPU time without any connection timeout coming to effect. This affects only HTTP/2 connections. A possible mitigation is to not enable the h2 protocol.

CVE-2016-4975 Medium (4.3)

Summary:Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the ”Location” or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).

CVE-2018-1283 Low (3.5)

Summary:In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to forward its session data to CGI applications (SessionEnv on, not the default), a remote user may influence their content by using a ”Session” header. This comes from the ”HTTP_SESSION” variable name used by mod_session to forward its data to CGIs, since the prefix ”HTTP_” is also used by the Apache HTTP Server to pass HTTP header fields, per CGI specifications.

CVE-2016-8612 Low (3.3)

Summary:Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process.

The above 28 vulnerabilities apply to these network locations:

- 192.168.0.15 Ports: ['80']

8 MySQL 5.5.5-10.3.20-MariaDB-0ubuntu0.19.04.1 (cpe:/a:mysql:mysql:5.5.5-10.3.20-mariadb-0ubuntu0.19.04.1)

NODEJS:602 Low (0.0)

Summary:

The above 1 vulnerabilities apply to these network locations:

- 192.168.0.16 Ports: ['3306']

Services With No Known Vulnerabilities

1 OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (cpe:/a:openbsd:openssh:7.2p2) (cpe:/o:linux:linux_ke

- 192.168.0.9 Ports: ['22']

2 ISC BIND 9.10.6-P1 (cpe:/a:isc:bind:9.10.6-p1)

- 192.168.0.11 Ports: ['53']

3 rpcbind

- 192.168.0.15 Ports: ['111']
- 192.168.0.11 Ports: ['111']

4 Jetty 9.4.22.v20191022 (cpe:/a:mortbay:jetty:9.4.22.v20191022)

- 192.168.0.13 Ports: ['8080']

5 tcpwrapped

- 192.168.0.15 Ports: ['7000']

6 OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (cpe:/a:openbsd:openssh:6.6.1p1) (cpe:/o:linux:linu

- 192.168.0.63 Ports: ['22']
- 192.168.0.5 Ports: ['22']
- 192.168.0.12 Ports: ['22']

7 domain

- 192.168.0.63 Ports: ['53']
- 192.168.0.5 Ports: ['53']
- 10.100.120.2 Ports: ['53']

8 MariaDB (cpe:/a:mariadb:mariadb)

- 192.168.0.15 Ports: ['3306']

9 OpenSSH 7.9p1 Ubuntu 10 (cpe:/a:openbsd:openssh:7.9p1) (cpe:/o:linux:linux_kernel)

- 192.168.0.13 Ports: ['22']
- 192.168.0.16 Ports: ['22']

10 ISC BIND 9.10.4-P1 (cpe:/a:isc:bind:9.10.4-p1)

- 192.168.0.15 Ports: ['53']

11 Samba smbd 3.X - 4.X (cpe:/a:samba:samba)

- 192.168.0.63 Ports: ['139', '445']
- 192.168.0.15 Ports: ['139', '445']
- 192.168.0.5 Ports: ['139', '445']

12 nginx (cpe:/a:igor_sysoev:nginx)

- 192.168.0.10 Ports: ['80']
- 10.100.120.2 Ports: ['80', '443']

13 irc

- 192.168.0.15 Ports: ['6667']

14 Sendmail 8.15.2/8.15.2 (cpe:/a:sendmail:sendmail:8.15.2%2F8.15.2)

- 192.168.0.15 Ports: ['25', '587']

15 Heimdal Kerberos (cpe:/a:heimdal:kerberos)

- 192.168.0.63 Ports: ['88']
- 192.168.0.5 Ports: ['88']

16 Microsoft Windows RPC (cpe:/o:microsoft:windows)

- 192.168.0.63 Ports: ['135', '1024']
- 192.168.0.5 Ports: ['135', '1024']

17 time

- 192.168.0.15 Ports: ['37']

18 ldap

- 192.168.0.63 Ports: ['389', '636', '3268', '3269']
- 192.168.0.5 Ports: ['389', '636', '3268', '3269']

19 vsftpd 3.0.3 (cpe:/a:vsftpd:vsftpd:3.0.3)

- 192.168.0.9 Ports: ['21']

20 afp

- 192.168.0.15 Ports: ['548']

21 printer

- 192.168.0.11 Ports: ['515']

22 ident

- 192.168.0.15 Ports: ['113']

23 kpasswd5

- 192.168.0.63 Ports: ['464']
- 192.168.0.5 Ports: ['464']

List of IPs Scanned

- 192.168.0.8
- 192.168.0.9
- 192.168.0.10
- 192.168.0.11
- 192.168.0.12
- 192.168.0.13
- 192.168.0.14
- 192.168.0.15
- 192.168.0.16
- 192.168.0.17
- 192.168.0.63
- 192.168.0.5
- 10.100.120.2
- 172.18.0.1

What we did after the scan

We could not close any ports as they are all being scored and are integral to our business funcitoning properly. For this reason, we have elected to not close any ports but rather patch our systems. For example, we saw that Apache and Samba were common services to be aflicted by the found CVEs, so we had to update our systems and harden our configuration files to ensure that our machines on the network are secure and are now patched against the vulnerabilities.