Отчет о сканировании периметра

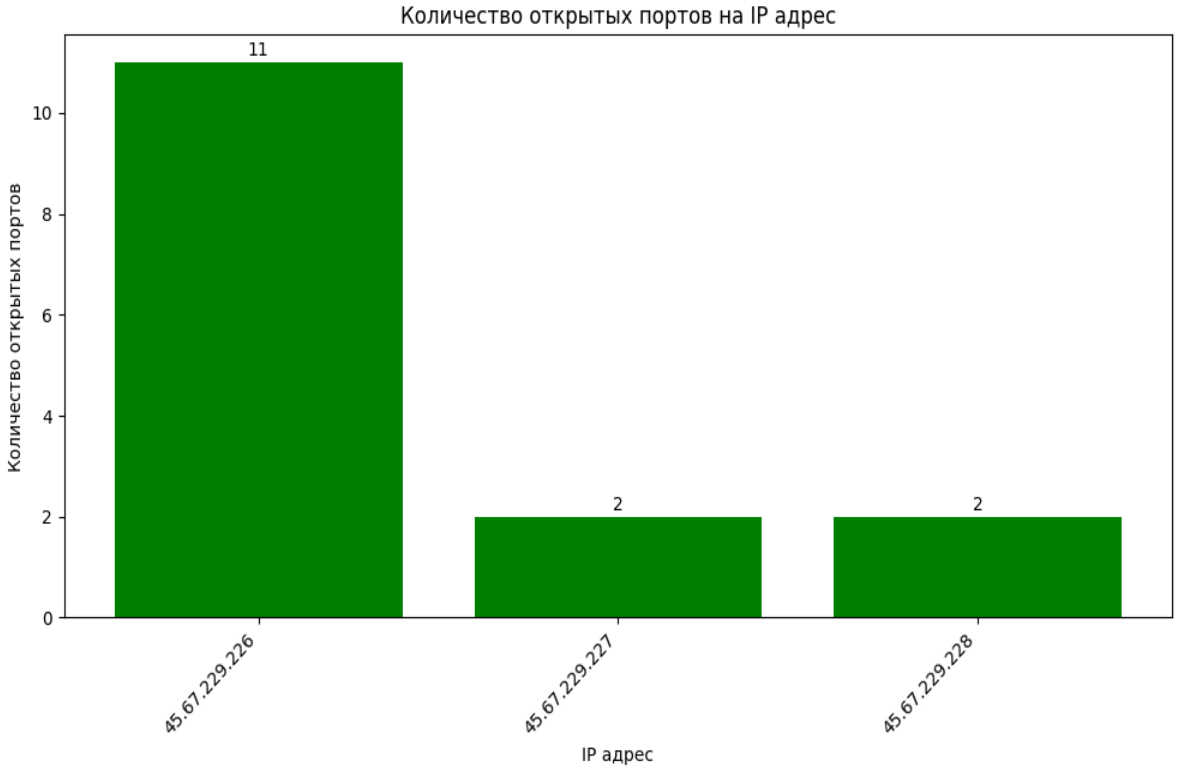
Были просканированы следующие ip-адреса: {'45.67.229.226', '45.67.229.228', '45.67.229.227'}

Были просканированы следующие порты: {(22, 'tcp'), (995, 'tcp'), (110, 'tcp'), (25, 'tcp'), (21, 'tcp'), (443, 'tcp'), (587, 'tcp'), (993, 'tcp'), (20, 'tcp'), (465, 'tcp'), (80, 'tcp'), (53, 'tcp'), (143, 'tcp')}

Сервисы, обнаруженные в сканируемом периметре: {('Exim smtpd', '4.92.3'), (None, None), ('OpenSSH', '7.4'), ('Dovecot imapd', None), ('ISC BIND', '9.11.4-P2'), ('Apache Traffic Server', None), ('Apache httpd', '2.4.6'), ('OpenSSH', '8.2p1 Ubuntu 4ubuntu0.5'), ('nginx', '1.25.4'), ('ProFTPD or KnFTPD', None), ('OpenSSH', '8.9p1 Ubuntu 3ubuntu0.10'), ('Dovecot pop3d', None)}

Количество найденных уязвимостей для каждого ip: {'45.67.229.226': 279, '45.67.229.227': 6, '45.67.229.228': 10}

Аналитическая информаиция


Количество открытых портов на IP адрес
Количество открытых портов
IP адрес
11
2
2
0
2
4
6
8
10
45.67.229.226
45.67.229.227
45.67.229.228


Распределение уязвимостей по уровням критичности
Критичный
20.3%
Информационный
0.0%
27.1%
Средний
52.5%
Высокий

Информация о портах и сервисах

IP-адрес	Имя хоста	Сервис/Версия	Порт/Протокол	Протокол L7	Статус порта
45.67.229.226	example.com	None/None	20/tcp	ftp-data	closed
45.67.229.226	example.com	ProFTPD or KnFTPD/None	21/tcp	ftp	open
45.67.229.226	example.com	OpenSSH/7.4	22/tcp	ssh	open
45.67.229.226	example.com	ISC BIND/9.11.4-P2	53/tcp	domain	open
45.67.229.226	example.com	Apache httpd/2.4.6	80/tcp	http	open
45.67.229.226	example.com	Dovecot pop3d/None	110/tcp	pop3	open
45.67.229.226	example.com	Dovecot imapd/None	143/tcp	imap	open
45.67.229.226	example.com	Apache httpd/2.4.6	443/tcp	http	open
45.67.229.226	example.com	Exim smtpd/4.92.3	465/tcp	smtp	open
45.67.229.226	example.com	Exim smtpd/4.92.3	587/tcp	smtp	open
45.67.229.226	example.com	None/None	993/tcp	imaps	open
45.67.229.226	example.com	None/None	995/tcp	pop3s	open
45.67.229.227	vm784790.stark-industries.solutions	OpenSSH/8.9p1 Ubuntu 3ubuntu0.10	22/tcp	ssh	open
45.67.229.227	vm784790.stark-industries.solutions	Apache Traffic Server/None	443/tcp	http-proxy	open
45.67.229.228	vm1557639.stark-industries.solutions	OpenSSH/8.2p1 Ubuntu 4ubuntu0.5	22/tcp	ssh	open
45.67.229.228	vm1557639.stark-industries.solutions	None/None	25/tcp	smtp	filtered
45.67.229.228	vm1557639.stark-industries.solutions	nginx/1.25.4	443/tcp	http	open

Информация об уязвимостях в сканируемом контуре

CVE	Имя хоста	Сервис/Версия	Порт/Протокол	CVSS V2	Описание
CVE-2023-38408	example.com	OpenSSH/7.4	22/tcp	9.8	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 o...
CVE-2020-15778	example.com	OpenSSH/7.4	22/tcp	7.8	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...

CVE-2021-41617	example.com	OpenSSH/7.4	22/tcp	7.0	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 gro...
CVE-2019-6110	example.com	OpenSSH/7.4	22/tcp	6.8	In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred....
CVE-2019-6109	example.com	OpenSSH/7.4	22/tcp	6.8	An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This af...

CVE-2023-51385	example.com	OpenSSH/7.4	22/tcp	6.5	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...
CVE-2023-48795	example.com	OpenSSH/7.4	22/tcp	5.9	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 connectio...
CVE-2020-14145	example.com	OpenSSH/7.4	22/tcp	5.9	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 sta...

CVE-2019-6111	example.com	OpenSSH/7.4	22/tcp	5.9	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)....
CVE-2018-20685	example.com	OpenSSH/7.4	22/tcp	5.3	In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side....
CVE-2018-15919	example.com	OpenSSH/7.4	22/tcp	5.3	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 "orac...

CVE-2018-15473	example.com	OpenSSH/7.4	22/tcp	5.3	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....
CVE-2017-15906	example.com	OpenSSH/7.4	22/tcp	5.3	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-2016-20012	example.com	OpenSSH/7.4	22/tcp	5.3	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: t...

CVE-2021-36368	example.com	OpenSSH/7.4	22/tcp	3.7	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 i...
CVE-2021-25216	example.com	ISC BIND/9.11.4-P2	53/tcp	9.8	In BIND 9.5.0 -> 9.11.29, 9.12.0 -> 9.16.13, and versions BIND 9.11.3-S1 -> 9.11.29-S1 and 9.16.8-S1 -> 9.16.13-S1 of BIND Supported Preview Edition, as well as release versions 9.17.0 -> 9.17.1 of the BIND 9.17 development branch, BIND servers are vulnerable if they are running an affected version ...
CVE-2020-8616	example.com	ISC BIND/9.11.4-P2	53/tcp	8.6	A malicious actor who intentionally exploits this lack of effective limitation on the number of fetches performed when processing referrals can, through the use of specially crafted referrals, cause a recursing server to issue a very large number of fetches in an attempt to process the referral. Thi...

CVE-2020-8625	example.com	ISC BIND/9.11.4-P2	53/tcp	8.1	BIND servers are vulnerable if they are running an affected version and are configured to use GSS-TSIG features. In a configuration which uses BIND's default settings the vulnerable code path is not exposed, but a server can be rendered vulnerable by explicitly setting valid values for the tkey-gssa...
CVE-2023-50387	example.com	ISC BIND/9.11.4-P2	53/tcp	7.5	Certain DNSSEC aspects of the DNS protocol (in RFC 4033, 4034, 4035, 6840, and related RFCs) allow remote attackers to cause a denial of service (CPU consumption) via one or more DNSSEC responses, aka the "KeyTrap" issue. One of the concerns is that, when there is a zone with many DNSKEY and RRSIG r...
CVE-2023-3341	example.com	ISC BIND/9.11.4-P2	53/tcp	7.5	The code that processes control channel messages sent to `named` calls certain functions recursively during packet parsing. Recursion depth is only limited by the maximum accepted packet size; depending on the environment, this may cause the packet-parsing code to run out of available stack memory, ...

CVE-2023-2828	example.com	ISC BIND/9.11.4-P2	53/tcp	7.5	Every `named` instance configured to run as a recursive resolver maintains a cache database holding the responses to the queries it has recently sent to authoritative servers. The size limit for that cache database can be configured using the `max-cache-size` statement in the configuration file; it ...
CVE-2022-38178	example.com	ISC BIND/9.11.4-P2	53/tcp	7.5	By spoofing the target resolver with responses that have a malformed EdDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources....
CVE-2022-38177	example.com	ISC BIND/9.11.4-P2	53/tcp	7.5	By spoofing the target resolver with responses that have a malformed ECDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources....

CVE-2022-3488	example.com	ISC BIND/9.11.4-P2	53/tcp	7.5	Processing of repeated responses to the same query, where both responses contain ECS pseudo-options, but where the first is broken in some way, can cause BIND to exit with an assertion failure. 'Broken' in this context is anything that would cause the resolver to reject the query response, such as ...
CVE-2021-25215	example.com	ISC BIND/9.11.4-P2	53/tcp	7.5	In BIND 9.0.0 -> 9.11.29, 9.12.0 -> 9.16.13, and versions BIND 9.9.3-S1 -> 9.11.29-S1 and 9.16.8-S1 -> 9.16.13-S1 of BIND Supported Preview Edition, as well as release versions 9.17.0 -> 9.17.11 of the BIND 9.17 development branch, when a vulnerable version of named receives a query for a record tri...
CVE-2020-8623	example.com	ISC BIND/9.11.4-P2	53/tcp	7.5	In BIND 9.10.0 -> 9.11.21, 9.12.0 -> 9.16.5, 9.17.0 -> 9.17.3, also affects 9.10.5-S1 -> 9.11.21-S1 of the BIND 9 Supported Preview Edition, An attacker that can reach a vulnerable system with a specially crafted query packet can trigger a crash. To be vulnerable, the system must: * be running BIND ...

CVE-2020-8617	example.com	ISC BIND/9.11.4-P2	53/tcp	7.5	Using a specially-crafted message, an attacker may potentially cause a BIND server to reach an inconsistent state if the attacker knows (or successfully guesses) the name of a TSIG key used by the server. Since BIND, by default, configures a local session key even on servers whose configuration does...
CVE-2019-6470	example.com	ISC BIND/9.11.4-P2	53/tcp	7.5	There had existed in one of the ISC BIND libraries a bug in a function that was used by dhcpd when operating in DHCPv6 mode. There was also a bug in dhcpd relating to the use of this function per its documentation, but the bug in the library function prevented this from causing any harm. All release...
CVE-2018-5744	example.com	ISC BIND/9.11.4-P2	53/tcp	7.5	A failure to free memory can occur when processing messages having a specific combination of EDNS options. Versions affected are: BIND 9.10.7 -> 9.10.8-P1, 9.11.3 -> 9.11.5-P1, 9.12.0 -> 9.12.3-P1, and versions 9.10.7-S1 -> 9.11.5-S3 of BIND 9 Supported Preview Edition. Versions 9.13.0 -> 9.13.6 of ...

CVE-2018-5743	example.com	ISC BIND/9.11.4-P2	53/tcp	7.5	By design, BIND is intended to limit the number of TCP clients that can be connected at any given time. The number of allowed connections is a tunable parameter which, if unset, defaults to a conservative value for most servers. Unfortunately, the code which was intended to limit the number of simul...
CVE-2021-25220	example.com	ISC BIND/9.11.4-P2	53/tcp	6.8	BIND 9.11.0 -> 9.11.36 9.12.0 -> 9.16.26 9.17.0 -> 9.18.0 BIND Supported Preview Editions: 9.11.4-S1 -> 9.11.36-S1 9.16.8-S1 -> 9.16.26-S1 Versions of BIND 9 earlier than those shown - back to 9.1.0, including Supported Preview Editions - are also believed to be affected but have not been tested as ...
CVE-2021-25214	example.com	ISC BIND/9.11.4-P2	53/tcp	6.5	In BIND 9.8.5 -> 9.8.8, 9.9.3 -> 9.11.29, 9.12.0 -> 9.16.13, and versions BIND 9.9.3-S1 -> 9.11.29-S1 and 9.16.8-S1 -> 9.16.13-S1 of BIND 9 Supported Preview Edition, as well as release versions 9.17.0 -> 9.17.11 of the BIND 9.17 development branch, when a vulnerable version of named receives a malf...

CVE-2020-8622	example.com	ISC BIND/9.11.4-P2	53/tcp	6.5	In BIND 9.0.0 -> 9.11.21, 9.12.0 -> 9.16.5, 9.17.0 -> 9.17.3, also affects 9.9.3-S1 -> 9.11.21-S1 of the BIND 9 Supported Preview Edition, An attacker on the network path for a TSIG-signed request, or operating the server receiving the TSIG-signed request, could send a truncated response to that req...
CVE-2018-5741	example.com	ISC BIND/9.11.4-P2	53/tcp	6.5	To provide fine-grained controls over the ability to use Dynamic DNS (DDNS) to update records in a zone, BIND 9 provides a feature called update-policy. Various rules can be configured to limit the types of updates that can be performed by a client, depending on the key used when sending the update ...
CVE-2019-6471	example.com	ISC BIND/9.11.4-P2	53/tcp	5.9	A race condition which may occur when discarding malformed packets can result in BIND exiting due to a REQUIRE assertion failure in dispatch.c. Versions affected: BIND 9.11.0 -> 9.11.7, 9.12.0 -> 9.12.4-P1, 9.14.0 -> 9.14.2. Also all releases of the BIND 9.13 development branch and version 9.15.0 of...

CVE-2022-2795	example.com	ISC BIND/9.11.4-P2	53/tcp	5.3	By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's performance, effectively denying legitimate clients access to the DNS resolution service....
CVE-2021-25219	example.com	ISC BIND/9.11.4-P2	53/tcp	5.3	In BIND 9.3.0 -> 9.11.35, 9.12.0 -> 9.16.21, and versions 9.9.3-S1 -> 9.11.35-S1 and 9.16.8-S1 -> 9.16.21-S1 of BIND Supported Preview Edition, as well as release versions 9.17.0 -> 9.17.18 of the BIND 9.17 development branch, exploitation of broken authoritative servers using a flaw in response pro...
CVE-2019-6465	example.com	ISC BIND/9.11.4-P2	53/tcp	5.3	Controls for zone transfers may not be properly applied to Dynamically Loadable Zones (DLZs) if the zones are writable Versions affected: BIND 9.9.0 -> 9.10.8-P1, 9.11.0 -> 9.11.5-P2, 9.12.0 -> 9.12.3-P2, and versions 9.9.3-S1 -> 9.11.5-S3 of BIND 9 Supported Preview Edition. Versions 9.13.0 -> 9.13...

CVE-2018-5745	example.com	ISC BIND/9.11.4-P2	53/tcp	4.9	"managed-keys" is a feature which allows a BIND resolver to automatically maintain the keys used by trust anchors which operators configure for use in DNSSEC validation. Due to an error in the managed-keys feature it is possible for a BIND server which uses managed-keys to exit due to an assertion f...
CVE-2020-8624	example.com	ISC BIND/9.11.4-P2	53/tcp	4.3	In BIND 9.9.12 -> 9.9.13, 9.10.7 -> 9.10.8, 9.11.3 -> 9.11.21, 9.12.1 -> 9.16.5, 9.17.0 -> 9.17.3, also affects 9.9.12-S1 -> 9.9.13-S1, 9.11.3-S1 -> 9.11.21-S1 of the BIND 9 Supported Preview Edition, An attacker who has been granted privileges to change a specific subset of the zone's content could...
CVE-2022-1665	example.com	ISC BIND/9.11.4-P2	53/tcp	8.2	A set of pre-production kernel packages of Red Hat Enterprise Linux for IBM Power architecture can be booted by the grub in Secure Boot mode even though it shouldn't. These kernel builds don't have the secure boot lockdown patches applied to it and can bypass the secure boot validations, allowing th...

CVE-2019-10143	example.com	ISC BIND/9.11.4-P2	53/tcp	7.0	It was discovered freeradius up to and including version 3.0.19 does not correctly configure logrotate, allowing a local attacker who already has control of the radiusd user to escalate his privileges to root, by tricking logrotate into writing a radiusd-writable file to a directory normally inacces...
CVE-2014-8181	example.com	ISC BIND/9.11.4-P2	53/tcp	5.5	The kernel in Red Hat Enterprise Linux 7 and MRG-2 does not clear garbage data for SG_IO buffer, which may leaking sensitive information to userspace....
CVE-2024-38476	example.com	Apache httpd/2.4.6	80/tcp	9.8	Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution via backend applications whose response headers are malicious or exploitable. Users are recommended to upgrade to version 2.4.60, which fixes this issue....

CVE-2024-38474	example.com	Apache httpd/2.4.6	80/tcp	9.8	Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts in directories permitted by the configuration but not directly reachable by any URL or source disclosure of scripts meant to only to be executed as CGI. Users are recommended to up...
CVE-2023-25690	example.com	Apache httpd/2.4.6	80/tcp	9.8	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-...
CVE-2022-31813	example.com	Apache httpd/2.4.6	80/tcp	9.8	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....

CVE-2022-23943	example.com	Apache httpd/2.4.6	80/tcp	9.8	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....
CVE-2022-22720	example.com	Apache httpd/2.4.6	80/tcp	9.8	Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling...
CVE-2021-44790	example.com	Apache httpd/2.4.6	80/tcp	9.8	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 earli...

CVE-2021-42013	example.com	Apache httpd/2.4.6	80/tcp	9.8	It was found that the fix for CVE-2021-41773 in Apache HTTP Server 2.4.50 was insufficient. An attacker could use a path traversal attack to map URLs to files outside the directories configured by Alias-like directives. If files outside of these directories are not protected by the usual default con...
CVE-2021-39275	example.com	Apache httpd/2.4.6	80/tcp	9.8	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....
CVE-2021-26691	example.com	Apache httpd/2.4.6	80/tcp	9.8	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...

CVE-2018-1312	example.com	Apache httpd/2.4.6	80/tcp	9.8	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...
CVE-2017-7679	example.com	Apache httpd/2.4.6	80/tcp	9.8	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-2017-3169	example.com	Apache httpd/2.4.6	80/tcp	9.8	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	example.com	Apache httpd/2.4.6	80/tcp	9.8	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-2024-38475	example.com	Apache httpd/2.4.6	80/tcp	9.1	Improper escaping of output in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows an attacker to map URLs to filesystem locations that are permitted to be served by the server but are not intentionally/directly reachable by any URL, resulting in code execution or source code disclosure. S...
CVE-2022-28615	example.com	Apache httpd/2.4.6	80/tcp	9.1	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_strcm...
CVE-2022-22721	example.com	Apache httpd/2.4.6	80/tcp	9.1	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....

CVE-2017-9788	example.com	Apache httpd/2.4.6	80/tcp	9.1	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 v...
CVE-2022-36760	example.com	Apache httpd/2.4.6	80/tcp	9.0	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 versio...
CVE-2021-40438	example.com	Apache httpd/2.4.6	80/tcp	9.0	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....

CVE-2024-38473	example.com	Apache httpd/2.4.6	80/tcp	8.1	Encoding problem in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows request URLs with incorrect encoding to be sent to backend services, potentially bypassing authentication via crafted requests. Users are recommended to upgrade to version 2.4.60, which fixes this issue....
CVE-2017-15715	example.com	Apache httpd/2.4.6	80/tcp	8.1	In Apache httpd 2.4.0 to 2.4.29, the expression specified in 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 mat...
CVE-2016-5387	example.com	Apache httpd/2.4.6	80/tcp	8.1	The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary p...

CVE-2024-40898	example.com	Apache httpd/2.4.6	80/tcp	7.5	SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests. Users are recommended to upgrade to version 2.4.62 which fixes this issue. ...
CVE-2024-39573	example.com	Apache httpd/2.4.6	80/tcp	7.5	Potential SSRF in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows an attacker to cause unsafe RewriteRules to unexpectedly setup URL's to be handled by mod_proxy. Users are recommended to upgrade to version 2.4.60, which fixes this issue....
CVE-2024-38477	example.com	Apache httpd/2.4.6	80/tcp	7.5	null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request. Users are recommended to upgrade to version 2.4.60, which fixes this issue....

CVE-2024-38472	example.com	Apache httpd/2.4.6	80/tcp	7.5	SSRF in Apache HTTP Server on Windows allows to potentially leak NTLM hashes to a malicious server via SSRF and malicious requests or content Users are recommended to upgrade to version 2.4.60 which fixes this issue. Note: Existing configurations that access UNC paths will have to configure new di...
CVE-2023-31122	example.com	Apache httpd/2.4.6	80/tcp	7.5	Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57. ...
CVE-2022-30556	example.com	Apache httpd/2.4.6	80/tcp	7.5	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....
CVE-2022-30522	example.com	Apache httpd/2.4.6	80/tcp	7.5	If Apache HTTP Server 2.4.53 is configured to do transformations with mod_sed in contexts where the input to mod_sed may be very large, mod_sed may make excessively large memory allocations and trigger an abort....

CVE-2022-29404	example.com	Apache httpd/2.4.6	80/tcp	7.5	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....
CVE-2022-26377	example.com	Apache httpd/2.4.6	80/tcp	7.5	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 version...
CVE-2022-22719	example.com	Apache httpd/2.4.6	80/tcp	7.5	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....

CVE-2021-41524	example.com	Apache httpd/2.4.6	80/tcp	7.5	While fuzzing the 2.4.49 httpd, a new null pointer dereference was detected during HTTP/2 request processing, allowing an external source to DoS the server. This requires a specially crafted request. The vulnerability was recently introduced in version 2.4.49. No exploit is known to the project....
CVE-2021-36160	example.com	Apache httpd/2.4.6	80/tcp	7.5	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)....
CVE-2021-34798	example.com	Apache httpd/2.4.6	80/tcp	7.5	Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier....
CVE-2021-33193	example.com	Apache httpd/2.4.6	80/tcp	7.5	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....

CVE-2021-31618	example.com	Apache httpd/2.4.6	80/tcp	7.5	Apache HTTP Server protocol handler for the HTTP/2 protocol checks received request headers against the size limitations as configured for the server and used for the HTTP/1 protocol as well. On violation of these restrictions and HTTP response is sent to the client with a status code indicating why...
CVE-2021-26690	example.com	Apache httpd/2.4.6	80/tcp	7.5	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...
CVE-2020-13950	example.com	Apache httpd/2.4.6	80/tcp	7.5	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...

CVE-2019-0217	example.com	Apache httpd/2.4.6	80/tcp	7.5	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....
CVE-2019-0215	example.com	Apache httpd/2.4.6	80/tcp	7.5	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-2019-0190	example.com	Apache httpd/2.4.6	80/tcp	7.5	A bug exists in the way mod_ssl handled client renegotiations. A remote attacker could send a carefully crafted request that would cause mod_ssl to enter a loop leading to a denial of service. This bug can be only triggered with Apache HTTP Server version 2.4.37 when using OpenSSL version 1.1.1 or l...

CVE-2018-8011	example.com	Apache httpd/2.4.6	80/tcp	7.5	By specially crafting HTTP requests, the mod_md challenge handler would dereference a NULL pointer and cause the child process to segfault. This could be used to DoS the server. Fixed in Apache HTTP Server 2.4.34 (Affected 2.4.33)....
CVE-2018-17199	example.com	Apache httpd/2.4.6	80/tcp	7.5	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	example.com	Apache httpd/2.4.6	80/tcp	7.5	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-2018-1303	example.com	Apache httpd/2.4.6	80/tcp	7.5	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. It could be used as a Denial of Service attack against users of mod_cache_socache. The vulnerability is considered...
CVE-2017-9798	example.com	Apache httpd/2.4.6	80/tcp	7.5	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...
CVE-2017-9789	example.com	Apache httpd/2.4.6	80/tcp	7.5	When under stress, closing many connections, the HTTP/2 handling code in Apache httpd 2.4.26 would sometimes access memory after it has been freed, resulting in potentially erratic behaviour....

CVE-2017-7668	example.com	Apache httpd/2.4.6	80/tcp	7.5	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...
CVE-2017-7659	example.com	Apache httpd/2.4.6	80/tcp	7.5	A maliciously constructed HTTP/2 request could cause mod_http2 in Apache HTTP Server 2.4.24, 2.4.25 to dereference a NULL pointer and crash the server process....
CVE-2017-15710	example.com	Apache httpd/2.4.6	80/tcp	7.5	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 conve...

CVE-2016-8743	example.com	Apache httpd/2.4.6	80/tcp	7.5	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 a...
CVE-2016-2161	example.com	Apache httpd/2.4.6	80/tcp	7.5	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	example.com	Apache httpd/2.4.6	80/tcp	7.5	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 oracl...

CVE-2006-20001	example.com	Apache httpd/2.4.6	80/tcp	7.5	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. ...
CVE-2023-38709	example.com	Apache httpd/2.4.6	80/tcp	7.3	Faulty input validation in the core of Apache allows malicious or exploitable backend/content generators to split HTTP responses. This issue affects Apache HTTP Server: through 2.4.58....
CVE-2020-35452	example.com	Apache httpd/2.4.6	80/tcp	7.3	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...

CVE-2014-0226	example.com	Apache httpd/2.4.6	80/tcp	6.8	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 ha...
CVE-2024-24795	example.com	Apache httpd/2.4.6	80/tcp	6.3	HTTP Response splitting in multiple modules in Apache HTTP Server allows an attacker that can inject malicious response headers into backend applications to cause an HTTP desynchronization attack. Users are recommended to upgrade to version 2.4.59, which fixes this issue....
CVE-2024-39884	example.com	Apache httpd/2.4.6	80/tcp	6.2	A regression in the core of Apache HTTP Server 2.4.60 ignores some use of the legacy content-type based configuration of handlers. "AddType" and similar configuration, under some circumstances where files are requested indirectly, result in source code disclosure of local content. For example, PHP...

CVE-2020-1927	example.com	Apache httpd/2.4.6	80/tcp	6.1	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....
CVE-2019-10098	example.com	Apache httpd/2.4.6	80/tcp	6.1	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-2019-10092	example.com	Apache httpd/2.4.6	80/tcp	6.1	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 prox...

CVE-2016-4975	example.com	Apache httpd/2.4.6	80/tcp	6.1	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....
CVE-2023-45802	example.com	Apache httpd/2.4.6	80/tcp	5.9	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 t...
CVE-2018-1302	example.com	Apache httpd/2.4.6	80/tcp	5.9	When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter an...

CVE-2018-1301	example.com	Apache httpd/2.4.6	80/tcp	5.9	A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level),...
CVE-2020-13938	example.com	Apache httpd/2.4.6	80/tcp	5.5	Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows...
CVE-2022-37436	example.com	Apache httpd/2.4.6	80/tcp	5.3	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....
CVE-2022-28614	example.com	Apache httpd/2.4.6	80/tcp	5.3	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 t...

CVE-2022-28330	example.com	Apache httpd/2.4.6	80/tcp	5.3	Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module....
CVE-2021-30641	example.com	Apache httpd/2.4.6	80/tcp	5.3	Apache HTTP Server versions 2.4.39 to 2.4.46 Unexpected matching behavior with 'MergeSlashes OFF'...
CVE-2020-1934	example.com	Apache httpd/2.4.6	80/tcp	5.3	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....
CVE-2020-11985	example.com	Apache httpd/2.4.6	80/tcp	5.3	IP address spoofing when proxying using mod_remoteip and mod_rewrite For configurations using proxying with mod_remoteip and certain mod_rewrite rules, an attacker could spoof their IP address for logging and PHP scripts. Note this issue was fixed in Apache HTTP Server 2.4.24 but was retrospectively...

CVE-2019-17567	example.com	Apache httpd/2.4.6	80/tcp	5.3	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, authenticatio...
CVE-2019-0220	example.com	Apache httpd/2.4.6	80/tcp	5.3	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 wil...
CVE-2018-1283	example.com	Apache httpd/2.4.6	80/tcp	5.3	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...

CVE-2015-3183	example.com	Apache httpd/2.4.6	80/tcp	5.0	The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension chara...
CVE-2015-0228	example.com	Apache httpd/2.4.6	80/tcp	5.0	The lua_websocket_read function in lua_request.c in the mod_lua module in the Apache HTTP Server through 2.4.12 allows remote attackers to cause a denial of service (child-process crash) by sending a crafted WebSocket Ping frame after a Lua script has called the wsupgrade function....
CVE-2014-3581	example.com	Apache httpd/2.4.6	80/tcp	5.0	The cache_merge_headers_out function in modules/cache/cache_util.c in the mod_cache module in the Apache HTTP Server before 2.4.11 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty HTTP Content-Type header....

CVE-2014-3523	example.com	Apache httpd/2.4.6	80/tcp	5.0	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	example.com	Apache httpd/2.4.6	80/tcp	5.0	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-2014-0098	example.com	Apache httpd/2.4.6	80/tcp	5.0	The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation....

CVE-2013-6438	example.com	Apache httpd/2.4.6	80/tcp	5.0	The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request....
CVE-2013-5704	example.com	Apache httpd/2.4.6	80/tcp	5.0	The mod_headers module in the Apache HTTP Server 2.2.22 allows remote attackers to bypass "RequestHeader unset" directives by placing a header in the trailer portion of data sent with chunked transfer coding. NOTE: the vendor states "this is not a security issue in httpd as such."...
CVE-2016-8612	example.com	Apache httpd/2.4.6	80/tcp	4.3	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....

CVE-2015-3185	example.com	Apache httpd/2.4.6	80/tcp	4.3	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 ...
CVE-2014-8109	example.com	Apache httpd/2.4.6	80/tcp	4.3	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 restrictio...
CVE-2014-0118	example.com	Apache httpd/2.4.6	80/tcp	4.3	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	example.com	Apache httpd/2.4.6	80/tcp	4.3	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-2013-4352	example.com	Apache httpd/2.4.6	80/tcp	4.3	The cache_invalidate function in modules/cache/cache_storage.c in the mod_cache module in the Apache HTTP Server 2.4.6, when a caching forward proxy is enabled, allows remote HTTP servers to cause a denial of service (NULL pointer dereference and daemon crash) via vectors that trigger a missing host...
CVE-2024-38476	example.com	Apache httpd/2.4.6	443/tcp	9.8	Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution via backend applications whose response headers are malicious or exploitable. Users are recommended to upgrade to version 2.4.60, which fixes this issue....

CVE-2024-38474	example.com	Apache httpd/2.4.6	443/tcp	9.8	Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts in directories permitted by the configuration but not directly reachable by any URL or source disclosure of scripts meant to only to be executed as CGI. Users are recommended to up...
CVE-2023-25690	example.com	Apache httpd/2.4.6	443/tcp	9.8	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-...
CVE-2022-31813	example.com	Apache httpd/2.4.6	443/tcp	9.8	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....

CVE-2022-23943	example.com	Apache httpd/2.4.6	443/tcp	9.8	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....
CVE-2022-22720	example.com	Apache httpd/2.4.6	443/tcp	9.8	Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling...
CVE-2021-44790	example.com	Apache httpd/2.4.6	443/tcp	9.8	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 earli...

CVE-2021-42013	example.com	Apache httpd/2.4.6	443/tcp	9.8	It was found that the fix for CVE-2021-41773 in Apache HTTP Server 2.4.50 was insufficient. An attacker could use a path traversal attack to map URLs to files outside the directories configured by Alias-like directives. If files outside of these directories are not protected by the usual default con...
CVE-2021-39275	example.com	Apache httpd/2.4.6	443/tcp	9.8	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....
CVE-2021-26691	example.com	Apache httpd/2.4.6	443/tcp	9.8	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...

CVE-2018-1312	example.com	Apache httpd/2.4.6	443/tcp	9.8	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...
CVE-2017-7679	example.com	Apache httpd/2.4.6	443/tcp	9.8	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-2017-3169	example.com	Apache httpd/2.4.6	443/tcp	9.8	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	example.com	Apache httpd/2.4.6	443/tcp	9.8	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-2024-38475	example.com	Apache httpd/2.4.6	443/tcp	9.1	Improper escaping of output in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows an attacker to map URLs to filesystem locations that are permitted to be served by the server but are not intentionally/directly reachable by any URL, resulting in code execution or source code disclosure. S...
CVE-2022-28615	example.com	Apache httpd/2.4.6	443/tcp	9.1	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_strcm...
CVE-2022-22721	example.com	Apache httpd/2.4.6	443/tcp	9.1	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....

CVE-2017-9788	example.com	Apache httpd/2.4.6	443/tcp	9.1	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 v...
CVE-2022-36760	example.com	Apache httpd/2.4.6	443/tcp	9.0	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 versio...
CVE-2021-40438	example.com	Apache httpd/2.4.6	443/tcp	9.0	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....

CVE-2024-38473	example.com	Apache httpd/2.4.6	443/tcp	8.1	Encoding problem in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows request URLs with incorrect encoding to be sent to backend services, potentially bypassing authentication via crafted requests. Users are recommended to upgrade to version 2.4.60, which fixes this issue....
CVE-2017-15715	example.com	Apache httpd/2.4.6	443/tcp	8.1	In Apache httpd 2.4.0 to 2.4.29, the expression specified in 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 mat...
CVE-2016-5387	example.com	Apache httpd/2.4.6	443/tcp	8.1	The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary p...

CVE-2024-40898	example.com	Apache httpd/2.4.6	443/tcp	7.5	SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests. Users are recommended to upgrade to version 2.4.62 which fixes this issue. ...
CVE-2024-39573	example.com	Apache httpd/2.4.6	443/tcp	7.5	Potential SSRF in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows an attacker to cause unsafe RewriteRules to unexpectedly setup URL's to be handled by mod_proxy. Users are recommended to upgrade to version 2.4.60, which fixes this issue....
CVE-2024-38477	example.com	Apache httpd/2.4.6	443/tcp	7.5	null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request. Users are recommended to upgrade to version 2.4.60, which fixes this issue....

CVE-2024-38472	example.com	Apache httpd/2.4.6	443/tcp	7.5	SSRF in Apache HTTP Server on Windows allows to potentially leak NTLM hashes to a malicious server via SSRF and malicious requests or content Users are recommended to upgrade to version 2.4.60 which fixes this issue. Note: Existing configurations that access UNC paths will have to configure new di...
CVE-2023-31122	example.com	Apache httpd/2.4.6	443/tcp	7.5	Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57. ...
CVE-2022-30556	example.com	Apache httpd/2.4.6	443/tcp	7.5	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....
CVE-2022-30522	example.com	Apache httpd/2.4.6	443/tcp	7.5	If Apache HTTP Server 2.4.53 is configured to do transformations with mod_sed in contexts where the input to mod_sed may be very large, mod_sed may make excessively large memory allocations and trigger an abort....

CVE-2022-29404	example.com	Apache httpd/2.4.6	443/tcp	7.5	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....
CVE-2022-26377	example.com	Apache httpd/2.4.6	443/tcp	7.5	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 version...
CVE-2022-22719	example.com	Apache httpd/2.4.6	443/tcp	7.5	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....

CVE-2021-41524	example.com	Apache httpd/2.4.6	443/tcp	7.5	While fuzzing the 2.4.49 httpd, a new null pointer dereference was detected during HTTP/2 request processing, allowing an external source to DoS the server. This requires a specially crafted request. The vulnerability was recently introduced in version 2.4.49. No exploit is known to the project....
CVE-2021-36160	example.com	Apache httpd/2.4.6	443/tcp	7.5	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)....
CVE-2021-34798	example.com	Apache httpd/2.4.6	443/tcp	7.5	Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier....
CVE-2021-33193	example.com	Apache httpd/2.4.6	443/tcp	7.5	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....

CVE-2021-31618	example.com	Apache httpd/2.4.6	443/tcp	7.5	Apache HTTP Server protocol handler for the HTTP/2 protocol checks received request headers against the size limitations as configured for the server and used for the HTTP/1 protocol as well. On violation of these restrictions and HTTP response is sent to the client with a status code indicating why...
CVE-2021-26690	example.com	Apache httpd/2.4.6	443/tcp	7.5	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...
CVE-2020-13950	example.com	Apache httpd/2.4.6	443/tcp	7.5	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...

CVE-2019-0217	example.com	Apache httpd/2.4.6	443/tcp	7.5	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....
CVE-2019-0215	example.com	Apache httpd/2.4.6	443/tcp	7.5	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-2019-0190	example.com	Apache httpd/2.4.6	443/tcp	7.5	A bug exists in the way mod_ssl handled client renegotiations. A remote attacker could send a carefully crafted request that would cause mod_ssl to enter a loop leading to a denial of service. This bug can be only triggered with Apache HTTP Server version 2.4.37 when using OpenSSL version 1.1.1 or l...

CVE-2018-8011	example.com	Apache httpd/2.4.6	443/tcp	7.5	By specially crafting HTTP requests, the mod_md challenge handler would dereference a NULL pointer and cause the child process to segfault. This could be used to DoS the server. Fixed in Apache HTTP Server 2.4.34 (Affected 2.4.33)....
CVE-2018-17199	example.com	Apache httpd/2.4.6	443/tcp	7.5	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	example.com	Apache httpd/2.4.6	443/tcp	7.5	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-2018-1303	example.com	Apache httpd/2.4.6	443/tcp	7.5	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. It could be used as a Denial of Service attack against users of mod_cache_socache. The vulnerability is considered...
CVE-2017-9798	example.com	Apache httpd/2.4.6	443/tcp	7.5	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...
CVE-2017-9789	example.com	Apache httpd/2.4.6	443/tcp	7.5	When under stress, closing many connections, the HTTP/2 handling code in Apache httpd 2.4.26 would sometimes access memory after it has been freed, resulting in potentially erratic behaviour....

CVE-2017-7668	example.com	Apache httpd/2.4.6	443/tcp	7.5	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...
CVE-2017-7659	example.com	Apache httpd/2.4.6	443/tcp	7.5	A maliciously constructed HTTP/2 request could cause mod_http2 in Apache HTTP Server 2.4.24, 2.4.25 to dereference a NULL pointer and crash the server process....
CVE-2017-15710	example.com	Apache httpd/2.4.6	443/tcp	7.5	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 conve...

CVE-2016-8743	example.com	Apache httpd/2.4.6	443/tcp	7.5	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 a...
CVE-2016-2161	example.com	Apache httpd/2.4.6	443/tcp	7.5	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	example.com	Apache httpd/2.4.6	443/tcp	7.5	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 oracl...

CVE-2006-20001	example.com	Apache httpd/2.4.6	443/tcp	7.5	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. ...
CVE-2023-38709	example.com	Apache httpd/2.4.6	443/tcp	7.3	Faulty input validation in the core of Apache allows malicious or exploitable backend/content generators to split HTTP responses. This issue affects Apache HTTP Server: through 2.4.58....
CVE-2020-35452	example.com	Apache httpd/2.4.6	443/tcp	7.3	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...

CVE-2014-0226	example.com	Apache httpd/2.4.6	443/tcp	6.8	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 ha...
CVE-2024-24795	example.com	Apache httpd/2.4.6	443/tcp	6.3	HTTP Response splitting in multiple modules in Apache HTTP Server allows an attacker that can inject malicious response headers into backend applications to cause an HTTP desynchronization attack. Users are recommended to upgrade to version 2.4.59, which fixes this issue....
CVE-2024-39884	example.com	Apache httpd/2.4.6	443/tcp	6.2	A regression in the core of Apache HTTP Server 2.4.60 ignores some use of the legacy content-type based configuration of handlers. "AddType" and similar configuration, under some circumstances where files are requested indirectly, result in source code disclosure of local content. For example, PHP...

CVE-2020-1927	example.com	Apache httpd/2.4.6	443/tcp	6.1	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....
CVE-2019-10098	example.com	Apache httpd/2.4.6	443/tcp	6.1	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-2019-10092	example.com	Apache httpd/2.4.6	443/tcp	6.1	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 prox...

CVE-2016-4975	example.com	Apache httpd/2.4.6	443/tcp	6.1	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....
CVE-2023-45802	example.com	Apache httpd/2.4.6	443/tcp	5.9	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 t...
CVE-2018-1302	example.com	Apache httpd/2.4.6	443/tcp	5.9	When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter an...

CVE-2018-1301	example.com	Apache httpd/2.4.6	443/tcp	5.9	A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level),...
CVE-2020-13938	example.com	Apache httpd/2.4.6	443/tcp	5.5	Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows...
CVE-2022-37436	example.com	Apache httpd/2.4.6	443/tcp	5.3	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....
CVE-2022-28614	example.com	Apache httpd/2.4.6	443/tcp	5.3	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 t...

CVE-2022-28330	example.com	Apache httpd/2.4.6	443/tcp	5.3	Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module....
CVE-2021-30641	example.com	Apache httpd/2.4.6	443/tcp	5.3	Apache HTTP Server versions 2.4.39 to 2.4.46 Unexpected matching behavior with 'MergeSlashes OFF'...
CVE-2020-1934	example.com	Apache httpd/2.4.6	443/tcp	5.3	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....
CVE-2020-11985	example.com	Apache httpd/2.4.6	443/tcp	5.3	IP address spoofing when proxying using mod_remoteip and mod_rewrite For configurations using proxying with mod_remoteip and certain mod_rewrite rules, an attacker could spoof their IP address for logging and PHP scripts. Note this issue was fixed in Apache HTTP Server 2.4.24 but was retrospectively...

CVE-2019-17567	example.com	Apache httpd/2.4.6	443/tcp	5.3	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, authenticatio...
CVE-2019-0220	example.com	Apache httpd/2.4.6	443/tcp	5.3	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 wil...
CVE-2018-1283	example.com	Apache httpd/2.4.6	443/tcp	5.3	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...

CVE-2015-3183	example.com	Apache httpd/2.4.6	443/tcp	5.0	The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension chara...
CVE-2015-0228	example.com	Apache httpd/2.4.6	443/tcp	5.0	The lua_websocket_read function in lua_request.c in the mod_lua module in the Apache HTTP Server through 2.4.12 allows remote attackers to cause a denial of service (child-process crash) by sending a crafted WebSocket Ping frame after a Lua script has called the wsupgrade function....
CVE-2014-3581	example.com	Apache httpd/2.4.6	443/tcp	5.0	The cache_merge_headers_out function in modules/cache/cache_util.c in the mod_cache module in the Apache HTTP Server before 2.4.11 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty HTTP Content-Type header....

CVE-2014-3523	example.com	Apache httpd/2.4.6	443/tcp	5.0	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	example.com	Apache httpd/2.4.6	443/tcp	5.0	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-2014-0098	example.com	Apache httpd/2.4.6	443/tcp	5.0	The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation....

CVE-2013-6438	example.com	Apache httpd/2.4.6	443/tcp	5.0	The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request....
CVE-2013-5704	example.com	Apache httpd/2.4.6	443/tcp	5.0	The mod_headers module in the Apache HTTP Server 2.2.22 allows remote attackers to bypass "RequestHeader unset" directives by placing a header in the trailer portion of data sent with chunked transfer coding. NOTE: the vendor states "this is not a security issue in httpd as such."...
CVE-2016-8612	example.com	Apache httpd/2.4.6	443/tcp	4.3	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....

CVE-2015-3185	example.com	Apache httpd/2.4.6	443/tcp	4.3	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 ...
CVE-2014-8109	example.com	Apache httpd/2.4.6	443/tcp	4.3	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 restrictio...
CVE-2014-0118	example.com	Apache httpd/2.4.6	443/tcp	4.3	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	example.com	Apache httpd/2.4.6	443/tcp	4.3	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-2013-4352	example.com	Apache httpd/2.4.6	443/tcp	4.3	The cache_invalidate function in modules/cache/cache_storage.c in the mod_cache module in the Apache HTTP Server 2.4.6, when a caching forward proxy is enabled, allows remote HTTP servers to cause a denial of service (NULL pointer dereference and daemon crash) via vectors that trigger a missing host...
CVE-2023-42115	example.com	Exim smtpd/4.92.3	465/tcp	9.8	Exim AUTH Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Exim. Authentication is not required to exploit this vulnerability. The specific flaw exists within the smtp service, which listens o...
CVE-2022-37452	example.com	Exim smtpd/4.92.3	465/tcp	9.8	Exim before 4.95 has a heap-based buffer overflow for the alias list in host_name_lookup in host.c when sender_host_name is set....

CVE-2020-28026	example.com	Exim smtpd/4.92.3	465/tcp	9.8	Exim 4 before 4.94.2 has Improper Neutralization of Line Delimiters, relevant in non-default configurations that enable Delivery Status Notification (DSN). Certain uses of ORCPT= can place a newline into a spool header file, and indirectly allow unauthenticated remote attackers to execute arbitrary ...
CVE-2020-28024	example.com	Exim smtpd/4.92.3	465/tcp	9.8	Exim 4 before 4.94.2 allows Buffer Underwrite that may result in unauthenticated remote attackers executing arbitrary commands, because smtp_ungetc was only intended to push back characters, but can actually push back non-character error codes such as EOF....
CVE-2020-28022	example.com	Exim smtpd/4.92.3	465/tcp	9.8	Exim 4 before 4.94.2 has Improper Restriction of Write Operations within the Bounds of a Memory Buffer. This occurs when processing name=value pairs within MAIL FROM and RCPT TO commands....
CVE-2020-28018	example.com	Exim smtpd/4.92.3	465/tcp	9.8	Exim 4 before 4.94.2 allows Use After Free in smtp_reset in certain situations that may be common for builds with OpenSSL....

CVE-2020-28021	example.com	Exim smtpd/4.92.3	465/tcp	8.8	Exim 4 before 4.94.2 has Improper Neutralization of Line Delimiters. An authenticated remote SMTP client can insert newline characters into a spool file (which indirectly leads to remote code execution as root) via AUTH= in a MAIL FROM command....
CVE-2023-42117	example.com	Exim smtpd/4.92.3	465/tcp	8.1	Exim Improper Neutralization of Special Elements Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Exim. Authentication is not required to exploit this vulnerability. The specific flaw exists within the smtp servic...
CVE-2023-42116	example.com	Exim smtpd/4.92.3	465/tcp	8.1	Exim SMTP Challenge Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Exim. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of ...
CVE-2020-28016	example.com	Exim smtpd/4.92.3	465/tcp	7.8	Exim 4 before 4.94.2 allows an off-by-two Out-of-bounds Write because "-F "" is mishandled by parse_fix_phrase....

CVE-2020-28015	example.com	Exim smtpd/4.92.3	465/tcp	7.8	Exim 4 before 4.94.2 has Improper Neutralization of Line Delimiters. Local users can alter the behavior of root processes because a recipient address can have a newline character....
CVE-2020-28013	example.com	Exim smtpd/4.92.3	465/tcp	7.8	Exim 4 before 4.94.2 allows Heap-based Buffer Overflow because it mishandles "-F '.('" on the command line, and thus may allow privilege escalation from any user to root. This occurs because of the interpretation of negative sizes in strncpy....
CVE-2020-28012	example.com	Exim smtpd/4.92.3	465/tcp	7.8	Exim 4 before 4.94.2 allows Exposure of File Descriptor to Unintended Control Sphere because rda_interpret uses a privileged pipe that lacks a close-on-exec flag....
CVE-2020-28011	example.com	Exim smtpd/4.92.3	465/tcp	7.8	Exim 4 before 4.94.2 allows Heap-based Buffer Overflow in queue_run via two sender options: -R and -S. This may cause privilege escalation from exim to root....

CVE-2020-28010	example.com	Exim smtpd/4.92.3	465/tcp	7.8	Exim 4 before 4.94.2 allows Out-of-bounds Write because the main function, while setuid root, copies the current working directory pathname into a buffer that is too small (on some common platforms)....
CVE-2020-28009	example.com	Exim smtpd/4.92.3	465/tcp	7.8	Exim 4 before 4.94.2 allows Integer Overflow to Buffer Overflow because get_stdinput allows unbounded reads that are accompanied by unbounded increases in a certain size variable. NOTE: exploitation may be impractical because of the execution time needed to overflow (multiple days)....
CVE-2020-28008	example.com	Exim smtpd/4.92.3	465/tcp	7.8	Exim 4 before 4.94.2 allows Execution with Unnecessary Privileges. Because Exim operates as root in the spool directory (owned by a non-root user), an attacker can write to a /var/spool/exim4/input spool header file, in which a crafted recipient address can indirectly lead to command execution....

CVE-2020-28007	example.com	Exim smtpd/4.92.3	465/tcp	7.8	Exim 4 before 4.94.2 allows Execution with Unnecessary Privileges. Because Exim operates as root in the log directory (owned by a non-root user), a symlink or hard link attack allows overwriting critical root-owned files anywhere on the filesystem....
CVE-2022-37451	example.com	Exim smtpd/4.92.3	465/tcp	7.5	Exim before 4.96 has an invalid free in pam_converse in auths/call_pam.c because store_free is not used after store_malloc....
CVE-2020-28025	example.com	Exim smtpd/4.92.3	465/tcp	7.5	Exim 4 before 4.94.2 allows Out-of-bounds Read because pdkim_finish_bodyhash does not validate the relationship between sig->bodyhash.len and b->bh.len; thus, a crafted DKIM-Signature header might lead to a leak of sensitive information from process memory....
CVE-2020-28023	example.com	Exim smtpd/4.92.3	465/tcp	7.5	Exim 4 before 4.94.2 allows Out-of-bounds Read. smtp_setup_msg may disclose sensitive information from process memory to an unauthenticated SMTP client....

CVE-2020-28019	example.com	Exim smtpd/4.92.3	465/tcp	7.5	Exim 4 before 4.94.2 has Improper Initialization that can lead to recursion-based stack consumption or other consequences. This occurs because use of certain getc functions is mishandled when a client uses BDAT instead of DATA....
CVE-2020-12783	example.com	Exim smtpd/4.92.3	465/tcp	7.5	Exim through 4.93 has an out-of-bounds read in the SPA authenticator that could result in SPA/NTLM authentication bypass in auths/spa.c and auths/auth-spa.c....
CVE-2020-28014	example.com	Exim smtpd/4.92.3	465/tcp	6.1	Exim 4 before 4.94.2 allows Execution with Unnecessary Privileges. The -oP option is available to the exim user, and allows a denial of service because root-owned files can be overwritten....
CVE-2023-42114	example.com	Exim smtpd/4.92.3	465/tcp	3.7	Exim NTLM Challenge Out-Of-Bounds Read Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of Exim. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of ...

CVE-2023-42119	example.com	Exim smtpd/4.92.3	465/tcp	3.1	Exim dnsdb Out-Of-Bounds Read Information Disclosure Vulnerability. This vulnerability allows network-adjacent attackers to disclose sensitive information on affected installations of Exim. Authentication is not required to exploit this vulnerability. The specific flaw exists within the smtp servic...
CVE-2023-42115	example.com	Exim smtpd/4.92.3	587/tcp	9.8	Exim AUTH Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Exim. Authentication is not required to exploit this vulnerability. The specific flaw exists within the smtp service, which listens o...
CVE-2022-37452	example.com	Exim smtpd/4.92.3	587/tcp	9.8	Exim before 4.95 has a heap-based buffer overflow for the alias list in host_name_lookup in host.c when sender_host_name is set....

CVE-2020-28026	example.com	Exim smtpd/4.92.3	587/tcp	9.8	Exim 4 before 4.94.2 has Improper Neutralization of Line Delimiters, relevant in non-default configurations that enable Delivery Status Notification (DSN). Certain uses of ORCPT= can place a newline into a spool header file, and indirectly allow unauthenticated remote attackers to execute arbitrary ...
CVE-2020-28024	example.com	Exim smtpd/4.92.3	587/tcp	9.8	Exim 4 before 4.94.2 allows Buffer Underwrite that may result in unauthenticated remote attackers executing arbitrary commands, because smtp_ungetc was only intended to push back characters, but can actually push back non-character error codes such as EOF....
CVE-2020-28022	example.com	Exim smtpd/4.92.3	587/tcp	9.8	Exim 4 before 4.94.2 has Improper Restriction of Write Operations within the Bounds of a Memory Buffer. This occurs when processing name=value pairs within MAIL FROM and RCPT TO commands....
CVE-2020-28018	example.com	Exim smtpd/4.92.3	587/tcp	9.8	Exim 4 before 4.94.2 allows Use After Free in smtp_reset in certain situations that may be common for builds with OpenSSL....

CVE-2020-28021	example.com	Exim smtpd/4.92.3	587/tcp	8.8	Exim 4 before 4.94.2 has Improper Neutralization of Line Delimiters. An authenticated remote SMTP client can insert newline characters into a spool file (which indirectly leads to remote code execution as root) via AUTH= in a MAIL FROM command....
CVE-2023-42117	example.com	Exim smtpd/4.92.3	587/tcp	8.1	Exim Improper Neutralization of Special Elements Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Exim. Authentication is not required to exploit this vulnerability. The specific flaw exists within the smtp servic...
CVE-2023-42116	example.com	Exim smtpd/4.92.3	587/tcp	8.1	Exim SMTP Challenge Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Exim. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of ...
CVE-2020-28016	example.com	Exim smtpd/4.92.3	587/tcp	7.8	Exim 4 before 4.94.2 allows an off-by-two Out-of-bounds Write because "-F "" is mishandled by parse_fix_phrase....

CVE-2020-28015	example.com	Exim smtpd/4.92.3	587/tcp	7.8	Exim 4 before 4.94.2 has Improper Neutralization of Line Delimiters. Local users can alter the behavior of root processes because a recipient address can have a newline character....
CVE-2020-28013	example.com	Exim smtpd/4.92.3	587/tcp	7.8	Exim 4 before 4.94.2 allows Heap-based Buffer Overflow because it mishandles "-F '.("' on the command line, and thus may allow privilege escalation from any user to root. This occurs because of the interpretation of negative sizes in strncpy....
CVE-2020-28012	example.com	Exim smtpd/4.92.3	587/tcp	7.8	Exim 4 before 4.94.2 allows Exposure of File Descriptor to Unintended Control Sphere because rda_interpret uses a privileged pipe that lacks a close-on-exec flag....
CVE-2020-28011	example.com	Exim smtpd/4.92.3	587/tcp	7.8	Exim 4 before 4.94.2 allows Heap-based Buffer Overflow in queue_run via two sender options: -R and -S. This may cause privilege escalation from exim to root....

CVE-2020-28010	example.com	Exim smtpd/4.92.3	587/tcp	7.8	Exim 4 before 4.94.2 allows Out-of-bounds Write because the main function, while setuid root, copies the current working directory pathname into a buffer that is too small (on some common platforms)....
CVE-2020-28009	example.com	Exim smtpd/4.92.3	587/tcp	7.8	Exim 4 before 4.94.2 allows Integer Overflow to Buffer Overflow because get_stdinput allows unbounded reads that are accompanied by unbounded increases in a certain size variable. NOTE: exploitation may be impractical because of the execution time needed to overflow (multiple days)....
CVE-2020-28008	example.com	Exim smtpd/4.92.3	587/tcp	7.8	Exim 4 before 4.94.2 allows Execution with Unnecessary Privileges. Because Exim operates as root in the spool directory (owned by a non-root user), an attacker can write to a /var/spool/exim4/input spool header file, in which a crafted recipient address can indirectly lead to command execution....

CVE-2020-28007	example.com	Exim smtpd/4.92.3	587/tcp	7.8	Exim 4 before 4.94.2 allows Execution with Unnecessary Privileges. Because Exim operates as root in the log directory (owned by a non-root user), a symlink or hard link attack allows overwriting critical root-owned files anywhere on the filesystem....
CVE-2022-37451	example.com	Exim smtpd/4.92.3	587/tcp	7.5	Exim before 4.96 has an invalid free in pam_converse in auths/call_pam.c because store_free is not used after store_malloc....
CVE-2020-28025	example.com	Exim smtpd/4.92.3	587/tcp	7.5	Exim 4 before 4.94.2 allows Out-of-bounds Read because pdkim_finish_bodyhash does not validate the relationship between sig->bodyhash.len and b->bh.len; thus, a crafted DKIM-Signature header might lead to a leak of sensitive information from process memory....
CVE-2020-28023	example.com	Exim smtpd/4.92.3	587/tcp	7.5	Exim 4 before 4.94.2 allows Out-of-bounds Read. smtp_setup_msg may disclose sensitive information from process memory to an unauthenticated SMTP client....

CVE-2020-28019	example.com	Exim smtpd/4.92.3	587/tcp	7.5	Exim 4 before 4.94.2 has Improper Initialization that can lead to recursion-based stack consumption or other consequences. This occurs because use of certain getc functions is mishandled when a client uses BDAT instead of DATA....
CVE-2020-12783	example.com	Exim smtpd/4.92.3	587/tcp	7.5	Exim through 4.93 has an out-of-bounds read in the SPA authenticator that could result in SPA/NTLM authentication bypass in auths/spa.c and auths/auth-spa.c....
CVE-2020-28014	example.com	Exim smtpd/4.92.3	587/tcp	6.1	Exim 4 before 4.94.2 allows Execution with Unnecessary Privileges. The -oP option is available to the exim user, and allows a denial of service because root-owned files can be overwritten....
CVE-2023-42114	example.com	Exim smtpd/4.92.3	587/tcp	3.7	Exim NTLM Challenge Out-Of-Bounds Read Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of Exim. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of ...

CVE-2023-42119	example.com	Exim smtpd/4.92.3	587/tcp	3.1	Exim dnsdb Out-Of-Bounds Read Information Disclosure Vulnerability. This vulnerability allows network-adjacent attackers to disclose sensitive information on affected installations of Exim. Authentication is not required to exploit this vulnerability. The specific flaw exists within the smtp servic...
CVE-2023-38408	vm784790.stark-industries.solutions	OpenSSH/8.9p1 Ubuntu 3ubuntu0.10	22/tcp	9.8	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 o...
CVE-2023-28531	vm784790.stark-industries.solutions	OpenSSH/8.9p1 Ubuntu 3ubuntu0.10	22/tcp	9.8	ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9....

CVE-2024-6387	vm784790.stark-industries.solutions	OpenSSH/8.9p1 Ubuntu 3ubuntu0.10	22/tcp	8.1	A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period....
CVE-2023-51385	vm784790.stark-industries.solutions	OpenSSH/8.9p1 Ubuntu 3ubuntu0.10	22/tcp	6.5	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...
CVE-2023-48795	vm784790.stark-industries.solutions	OpenSSH/8.9p1 Ubuntu 3ubuntu0.10	22/tcp	5.9	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 connectio...

CVE-2023-51384	vm784790.stark-industries.solutions	OpenSSH/8.9p1 Ubuntu 3ubuntu0.10	22/tcp	5.5	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....
CVE-2023-38408	vm1557639.stark-industries.solutions	OpenSSH/8.2p1 Ubuntu 4ubuntu0.5	22/tcp	9.8	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 o...
CVE-2020-15778	vm1557639.stark-industries.solutions	OpenSSH/8.2p1 Ubuntu 4ubuntu0.5	22/tcp	7.8	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...

CVE-2020-12062	vm1557639.stark-industries.solutions	OpenSSH/8.2p1 Ubuntu 4ubuntu0.5	22/tcp	7.5	The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remo...
CVE-2021-28041	vm1557639.stark-industries.solutions	OpenSSH/8.2p1 Ubuntu 4ubuntu0.5	22/tcp	7.1	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....
CVE-2021-41617	vm1557639.stark-industries.solutions	OpenSSH/8.2p1 Ubuntu 4ubuntu0.5	22/tcp	7.0	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 gro...

CVE-2023-51385	vm1557639.stark-industries.solutions	OpenSSH/8.2p1 Ubuntu 4ubuntu0.5	22/tcp	6.5	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...
CVE-2023-48795	vm1557639.stark-industries.solutions	OpenSSH/8.2p1 Ubuntu 4ubuntu0.5	22/tcp	5.9	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 connectio...
CVE-2020-14145	vm1557639.stark-industries.solutions	OpenSSH/8.2p1 Ubuntu 4ubuntu0.5	22/tcp	5.9	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 sta...

CVE-2016-20012	vm1557639.stark-industries.solutions	OpenSSH/8.2p1 Ubuntu 4ubuntu0.5	22/tcp	5.3	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: t...
CVE-2021-36368	vm1557639.stark-industries.solutions	OpenSSH/8.2p1 Ubuntu 4ubuntu0.5	22/tcp	3.7	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 i...