https://siteprotector.io

Сводный отчет

SiteProtector.io запустил сканирование: Wed May 26 08:47:53 2021
Список просканированных адресов:

1. 37.140.192.112 Chkz.ru

Всего найдено открытых уязвимостей:

Сервисы с обнаруженными открытыми уязвимостями:

1. **Apache httpd 2.4.6 (cpe:/a:apache:http_server:2.4.6)**

Найдено 70 открытых уязвимостей для сервиса:

37.140.192.112 Открытые порты: [8081]

CVE-2017-7679 Critical (7.5)

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-2017-3167 Critical (7.5)

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.

PACKETSTORM:127546 High (6.8)

MSF:ILITIES/GENTOO-LINUX-CVE-2014-0226/ High (6.8)

EDB-ID:34133 High (6.8)

CVE-2018-1312 High (6.8)

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 servers by an attacker without detection.

CVE-2017-15715 High (6.8)

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

CVE-2014-0226 High (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 handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

1337DAY-ID-22451 High (6.8)

CVE-2017-9788 High (6.4)

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

MSF:ILITIES/REDHAT_LINUX-CVE-2019-0217/ High (6.0)

MSF:ILITIES/IBM-HTTP_SERVER-CVE-2019-0217/ High (6.0)

CVE-2019-0217 High (6.0)

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.

EDB-ID:47689 Medium (5.8)

CVE-2020-1927 Medium (5.8)

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 Medium (5.8)

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.

1337DAY-ID-33577 Medium (5.8)

CVE-2016-5387 Medium (5.1)

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 proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "This mitigation has been assigned the identifier CVE-2016-5387"; in other words, this is not a CVE ID for a vulnerability.

SSV:96537 Medium (5.0)

SSV:61874 Medium (5.0)

MSF:ILITIES/SUSE-CVE-2014-0231/ Medium (5.0)

MSF:AUXILIARY/SCANNER/HTTP/APACHE_OPTIONSBLEED Medium (5.0)

EXPLOITPACK:DAED9B9E8D259B28BF72FC7FDC4755A7 Medium (5.0)

EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D Medium (5.0)

CVE-2020-1934 Medium (5.0)

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-2019-0220 Medium (5.0)

A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.

CVE-2018-17199 Medium (5.0)

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-2018-17189 Medium (5.0)

In Apache HTTP server versions 2.4.37 and prior, by sending request bodies in a slow loris way to plain resources, the h2 stream for that request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 (mod_http2) connections.

CVE-2018-1303 Medium (5.0)

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 as low risk since mod_cache_socache is not widely used, mod_cache_disk is not concerned by this vulnerability.

CVE-2017-9798 Medium (5.0)

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

CVE-2017-15710 Medium (5.0)

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

CVE-2016-8743 Medium (5.0)

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

CVE-2016-2161 Medium (5.0)

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

CVE-2016-0736 Medium (5.0)

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

CVE-2015-3183 Medium (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 characters in modules/http/http_filters.c.

CVE-2015-0228 Medium (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-2014-3523 Medium (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 Medium (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 Medium (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 Medium (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.

1337DAY-ID-28573 Medium (5.0)

1337DAY-ID-26574 Medium (5.0)

SSV:87152 Medium (4.3)

PACKETSTORM:127563 Medium (4.3)

MSF:ILITIES/SUSE-CVE-2014-0118/ Medium (4.3)

MSF:ILITIES/SUSE-CVE-2013-4352/ Medium (4.3)

MSF:ILITIES/APACHE-HTTPD-CVE-2020-11985/ Medium (4.3)

MSF:ILITIES/AMAZON-LINUX-AMI-ALAS-2014-389/ Medium (4.3)

MSF:ILITIES/ALPINE-LINUX-CVE-2014-0117/ Medium (4.3)

EDB-ID:47688 Medium (4.3)

CVE-2020-11985 Medium (4.3)

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 allocated a low severity CVE in 2020.

CVE-2019-10092 Medium (4.3)

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

CVE-2018-1302 Medium (4.3)

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 and the team could not reproduce it outside debug builds, so it is classified as low risk.

CVE-2018-1301 Medium (4.3)

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), so it is classified as low risk for common server usage.

CVE-2016-4975 Medium (4.3)

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

CVE-2015-3185 Medium (4.3)

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

CVE-2014-8109 Medium (4.3)

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

CVE-2014-0118 Medium (4.3)

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

CVE-2014-0117 Medium (4.3)

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 Medium (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 hostname value.

1337DAY-ID-33575 Medium (4.3)

CVE-2018-1283 Medium (3.5)

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

CVE-2016-8612 Medium (3.3)

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.

PACKETSTORM:140265 Low (0.0)

EDB-ID:42745 Low (0.0)

EDB-ID:40961 Low (0.0)

1337DAY-ID-601 Low (0.0)

1337DAY-ID-2237 Low (0.0)

1337DAY-ID-1415 Low (0.0)

1337DAY-ID-1161 Low (0.0)

Сервисы без открытых уязвимостей:

rpcbind

37.140.192.112 Открытые порты: [111]

Dovecot imapd (cpe:/a:dovecot:dovecot)

37.140.192.112 Открытые порты: [143, 993]

MySQL 5.7.27-30 (cpe:/a:mysql:mysql:5.7.27-30)

37.140.192.112 Открытые порты: [3306]

Dropbear sshd 2019.78 (cpe:/a:matt_johnston:dropbear_ssh_server:2019.78) (cpe:/o:linux:linux_kernel)

37.140.192.112 Открытые порты: [22]

ISC BIND 9.11.4-P2 (cpe:/a:isc:bind:9.11.4-p2) (cpe:/o:redhat:enterprise_linux:7)

37.140.192.112 Открытые порты: [53]

ProFTPD or KnFTPD

37.140.192.112 Открытые порты: [21]

smtp

37.140.192.112 Открытые порты: [25]

vlsi-lm

37.140.192.112 Открытые порты: [1500]

Exim smtpd 4.94.2 (cpe:/a:exim:exim:4.94.2)

37.140.192.112 Открытые порты: [465, 587]

nginx (cpe:/a:igor_sysoev:nginx)

37.140.192.112 Открытые порты: [80, 443]

Dovecot pop3d (cpe:/a:dovecot:dovecot)

37.140.192.112 Открытые порты: [110, 995]