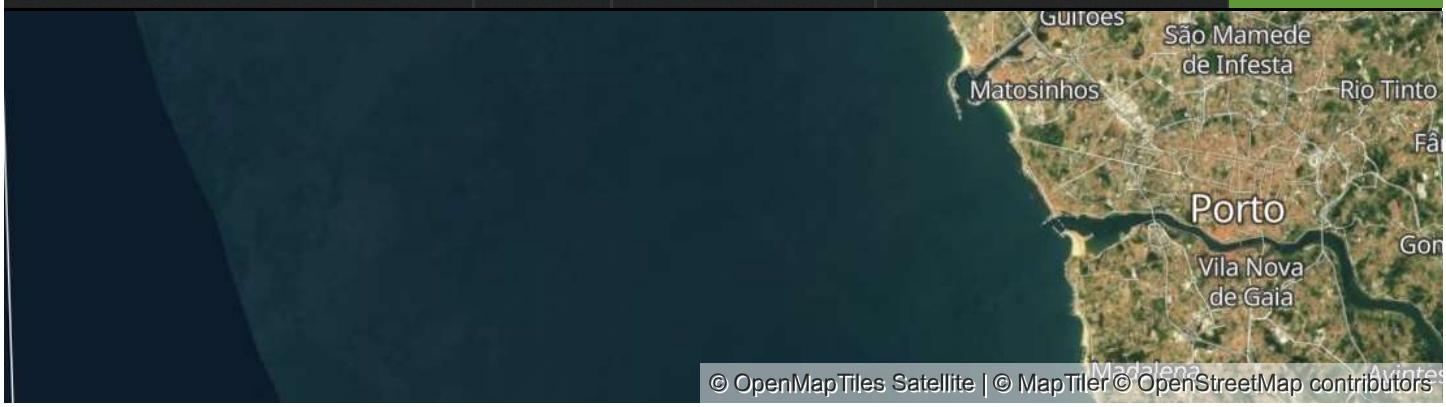

193.137.28.238

City	Porto
Country	Portugal
Organization	Universidade do Porto
ISP	Fundacao para a Ciencia e a Tecnologia, I.P.
Last Update	2020-03-03T05:11:25.104203
ASN	AS1930

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2014-0117	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-2017-15906	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-2014-0118	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-2016-0736	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-2015-3185	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-2015-3184	mod_authz_svn in Apache Subversion 1.7.x before 1.7.21 and 1.8.x before 1.8.14, when using Apache httpd 2.4.x, does not properly restrict anonymous access, which allows remote anonymous users to read hidden files via the path name.
CVE-2018-1312	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-2014-0098	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-2016-8612	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-2014-0226	Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.
CVE-2014-3523	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-2017-15710	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-2017-15715	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-2013-6438	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-2017-7679	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.
CVE-2018-17199	In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.

CVE-2017-9788	In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.
CVE-2014-8109	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-2017-9798	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-2016-2161	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-2018-15919	Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'
CVE-2014-0231	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-2013-4352	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.
CVE-2019-0220	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-2016-4975	Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).
CVE-2018-1283	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-2016-8743	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.

Ports

22 80 443

Services

22
tcp
ssh

OpenSSH Version: 7.4

```
SSH-2.0-OpenSSH_7.4
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDlUaGaS4q/b6BozHQ9CzWFVyQk+1IDLPvAa8hgTX41digU
yMeah5sQRKxewajRMor0rXcWcF6rlQojIE2cWxI3s/H1pVAZ6UATKDWF5WYUk0dkdTXQJ/Iq3fLX
19Qy4ega1l09GMt2KHRfhAWl0zHsK0W4cSTJCsALc9Z3Y6Nwn32XEGico5GPe8CVjiSnPpPIo6BT
9sIFdAKORse71wYUjSlMXK72fgWaZiInmWFmPmZQf9uYEkswwGnkKal8ywg930i8sPAqQkyHhtMI
rTVWAokYxGD8ILjQP1qJI90f4dmqPKtenOFJicvbEsAsCpobtmqr0PhoNTEnfVTdAteP
Fingerprint: 5c:92:3f:38:60:b2:57:32:80:d2:f0:5a:de:a6:3a:f1

Kex Algorithms:
        curve25519-sha256
        curve25519-sha256@libssh.org
        ecdh-sha2-nistp256
        ecdh-sha2-nistp384
        ecdh-sha2-nistp521
        diffie-hellman-group-exchange-sha256
        diffie-hellman-group16-sha512
        diffie-hellman-group18-sha512
        diffie-hellman-group-exchange-sha1
        diffie-hellman-group14-sha256
        diffie-hellman-group14-sha1
        diffie-hellman-group1-sha1

Server Host Key Algorithms:
        ssh-rsa
        rsa-sha2-512
        rsa-sha2-256
        ecdsa-sha2-nistp256

Encryption Algorithms:
        chacha20-poly1305@openssh.com
        aes128-ctr
        aes192-ctr
        aes256-ctr
        aes128-gcm@openssh.com
        aes256-gcm@openssh.com

MAC Algorithms:
        umac-64-etm@openssh.com
```

```
                umac-128-etm@openssh.com
                hmac-sha2-256-etm@openssh.com
                hmac-sha2-512-etm@openssh.com
                hmac-sha1-etm@openssh.com
                umac-64@openssh.com
                umac-128@openssh.com
                hmac-sha2-256
                hmac-sha2-512
                hmac-sha1

        Compression Algorithms:
                none
                zlib@openssh.com
```

80
tcp
http

Apache httpd Version: 2.4.6

```
HTTP/1.1 302 Found
Date: Fri, 28 Feb 2020 01:52:08 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips SVN/1.7.14 PHP/7.0.33
Location: https://www.omst.pt/
Content-Length: 204
Content-Type: text/html; charset=iso-8859-1
```

443
tcp
https

Apache httpd Version: 2.4.6

```
HTTP/1.1 200 OK
Date: Sat, 29 Feb 2020 04:02:42 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips SVN/1.7.14 PHP/7.0.33
Last-Modified: Mon, 13 Apr 2015 23:13:00 GMT
ETag: "0-513a34156189d"
Accept-Ranges: bytes
Content-Length: 0
Content-Type: text/html; charset=UTF-8
```

SSL Certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            03:dc:09:ba:3c:99:fe:56:94:84:cb:87:47:8f:54:ee:9f:b8
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
        Validity
            Not Before: Jan  4 21:18:50 2020 GMT
            Not After : Apr  3 21:18:50 2020 GMT
        Subject: CN=www.omst.pt
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
```

```
                Modulus:
                    00:ea:3f:f9:5e:00:fa:c2:b1:11:c5:2a:98:e3:6a:
                    ab:b9:72:76:84:a3:1a:84:bf:e8:f5:b0:c3:63:df:
                    71:02:0c:70:9f:46:e7:0b:33:fc:0d:3b:bd:94:78:
                    1a:5a:10:ae:99:eb:78:71:b5:a8:dc:bd:24:5b:2d:
                    f5:92:9b:b1:86:f6:47:f1:22:ed:57:9e:52:37:30:
                    74:f4:83:d3:52:a0:05:c2:c3:b2:fb:8c:33:61:ed:
                    98:6a:7d:31:07:7e:f9:ba:bf:21:4e:4e:f0:d7:7a:
                    bf:55:8a:e5:95:62:73:0e:91:84:7f:21:d6:34:2b:
                    85:5b:cc:04:0f:b4:6c:a0:fa:5f:f5:94:11:a9:83:
                    8e:91:d9:0e:2d:29:67:01:31:40:8c:e4:90:12:f7:
                    13:12:bc:bd:34:22:47:8d:e9:ab:13:97:7e:e5:97:
                    18:66:75:9a:d5:89:65:fe:ed:53:b8:cf:4d:03:8e:
                    5e:17:39:4c:cc:f6:ad:89:3d:e2:93:ec:a4:84:fb:
                    46:8a:6d:b8:4b:09:a1:0c:1e:12:4f:0b:15:e5:a8:
                    dc:bf:1a:73:b9:13:ba:91:c0:66:a0:2f:c6:c6:cc:
                    60:f0:67:02:1f:ea:61:c1:fa:3f:45:10:d8:5e:fe:
                    98:7f:85:44:51:cb:23:bb:06:9f:af:ab:28:fc:28:
                    f3:51
                Exponent: 65537 (0x10001)
            X509v3 extensions:
                X509v3 Key Usage: critical
                    Digital Signature, Key Encipherment
                X509v3 Extended Key Usage:
                    TLS Web Server Authentication, TLS Web Client Authentication
                X509v3 Basic Constraints: critical
                    CA:FALSE
                X509v3 Subject Key Identifier:
                    56:64:8B:C9:FB:28:C0:AE:16:39:8E:31:0F:7D:BE:44:00:00:7C:8F
                X509v3 Authority Key Identifier:
                    keyid:A8:4A:6A:63:04:7D:DD:BA:E6:D1:39:B7:A6:45:65:EF:F3:A8:EC:A1

                Authority Information Access:
                    OCSP - URI:http://ocsp.int-x3.letsencrypt.org
                    CA Issuers - URI:http://cert.int-x3.letsencrypt.org/

                X509v3 Subject Alternative Name:
                    DNS:www.omst.pt
                X509v3 Certificate Policies:
                    Policy: 2.23.140.1.2.1
                    Policy: 1.3.6.1.4.1.44947.1.1.1
                      CPS: http://cps.letsencrypt.org

                1.3.6.1.4.1.11129.2.4.2:
                    ......w.^.s..V...6H}.I.2z.........u..qEX...or........H0F.!..}|..h..t..!.`.....t...
8...\N..i.!..3...^.p66b....;.!...z.c0g.R.....v..... N.f.+..% gk..p..IS-...^...or........G0E. m.
`...l.....l...._V..<.m.Sw..e(..!....jq/....6.D....!..![
P/V...c.F
    Signature Algorithm: sha256WithRSAEncryption
         65:27:72:2d:ef:db:96:01:63:24:97:81:27:2a:08:a2:14:9c:
         f4:43:cd:05:5b:92:16:e2:8c:cf:08:19:62:21:f0:5b:36:77:
         d8:19:aa:90:99:be:e1:f4:7e:13:6f:cb:ee:85:85:fe:c8:da:
         c9:90:f8:e4:be:cd:8b:11:d9:92:ba:c0:41:49:3e:e2:c6:8f:
         5b:f8:93:6b:e0:3b:1c:31:29:5b:dd:b7:38:6b:e8:85:97:c7:
         f5:04:43:26:3f:33:d4:36:a1:30:9d:e8:6c:8d:77:e4:70:ae:
         d7:2b:ff:8b:d2:69:39:a4:84:7c:0f:99:5a:0e:5e:7b:6c:08:
         b6:45:9f:60:02:e8:30:bb:19:c1:ce:a4:d7:59:7e:f2:fc:e1:
         39:9b:43:e9:d4:1c:98:1c:14:37:cb:03:20:67:0c:e8:dc:30:
         cc:e9:a8:0a:8b:de:f4:12:97:63:0b:b9:da:ca:53:fa:28:00:
```

```
31:97:36:d5:01:ae:6b:27:65:ca:f0:d6:75:02:ba:fe:c3:0e:
04:a6:d7:51:1c:60:73:ed:e4:3a:37:83:7b:14:81:59:ea:64:
48:17:93:5d:27:e1:41:21:a5:3b:3f:84:4a:4f:f5:ba:a6:ed:
d7:19:b6:c5:b1:b4:ea:f2:9c:84:ac:fd:78:77:fb:a5:9a:7a:
0e:36:ec:02
```