Shodan | Maps | Images | Monitor | Developer | More...

SHODAN | Explore | Pricing | Search... | Login

76.133.182.10

Regular View   >_ Raw Data

© OpenMapTiles Satellite | © MapTiler © OpenStreetMap contributors

// LAST SEEN: 2024-05-26

General Information

Hostnames	c-76-133-182-10.hsd1.ca.**comcast.net** chatbot8.**steelrabbit.com**
Domains	COMCAST.NET STEELRABBIT.COM
Country	**United States**
City	**Hayward**
Organization	**Comcast Cable Communications, LLC**

Open **Ports**

443

// **443** / TCP

1149933577 | 2024-05-26T17:03:44.668874

Apache httpd 2.4.52

```
HTTP/1.1 200 OK
Date: Sun, 26 May 2024 17:03:44 GMT
Server: Apache/2.4.52 (Ubuntu)
Content-Length: 2513
Vary: Accept-Encoding
Content-Type: text/html; charset=utf-8
```

SSL Certificate

ISP	**Comcast Cable Communications, LLC**
ASN	**AS7922**

⚠ Vulnerabilities

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

CVE-2023-45802 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 the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that. This was found by the reporter during testing of CVE-2023-44487 (HTTP/2

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            04:a0:d7:ca:e7:3e:1b:c8:35:98:ef:a8:a5:e3:ef:db:c4:18
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Let's Encrypt, CN=R3
        Validity
            Not Before: Apr 17 01:08:32 2024 GMT
            Not After : Jul 16 01:08:31 2024 GMT
        Subject: CN=chatbot8.steelrabbit.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:bd:6b:94:b1:3f:ec:87:86:e4:8e:1c:c6:92:95:
                    0d:cc:b2:c1:64:5c:60:5c:01:5c:61:a6:07:8a:7f:
                    c8:95:c7:54:e3:6c:f1:60:4a:58:c3:f2:15:9b:e8:
                    1c:44:4d:3a:3a:16:17:50:78:9f:32:86:01:4d:f8:
                    67:1e:72:6a:bc:82:04:08:20:b4:7c:fe:7b:47:58:
                    73:50:e6:e3:d8:de:bf:c8:df:d2:65:e5:16:f8:57:
                    c8:0d:e6:0b:a2:8e:27:d5:13:59:8b:34:6d:bc:0f:
                    47:f1:06:8d:0b:53:35:3d:70:7c:be:80:10:73:7b:
                    c4:87:98:d3:6a:fa:23:93:17:ce:a3:0d:a9:3e:75:
                    e5:c8:fa:98:6f:27:26:18:cd:f4:d2:be:6c:88:5a:
                    f1:9c:08:5b:a3:13:a1:12:fd:49:bd:1f:54:a1:8a:
                    9f:2e:54:ed:b3:0a:f7:a7:54:a4:2e:85:0a:ea:96:
                    bd:97:df:a1:d5:5b:2b:89:0f:b3:48:74:fa:ad:21:
                    78:25:a5:26:d0:20:d0:98:11:50:fa:24:9b:a5:fa:
                    64:02:ee:68:65:29:ef:ef:4c:6d:de:71:f1:71:89:
                    0b:7c:7c:fd:16:67:7d:5b:94:af:3a:09:0e:88:33:
                    ac:36:be:8f:78:5e:d5:a1:9d:f7:f4:a2:c4:f3:ca:
                    ec:69
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Auth
entication
```

	Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out. Users are recommended to upgrade to version 2.4.58, which fixes the issue.
CVE-2023-31122	Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.
CVE-2023-27522	HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55. Special characters in the origin response header can truncate/split the response forwarded to the client.
CVE-2023-25690	Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.

```
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Subject Key Identifier:
                70:23:CE:A4:C1:40:4B:72:07:CF:2E:DF:77:82:EB:28:4
F:D3:C1:16
            X509v3 Authority Key Identifier:
                14:2E:B3:17:B7:58:56:CB:AE:50:09:40:E6:1F:AF:9D:8
B:14:C2:C6
            Authority Information Access:
                OCSP - URI:http://r3.o.lencr.org
                CA Issuers - URI:http://r3.i.lencr.org/
            X509v3 Subject Alternative Name:
                DNS:chatbot8.steelrabbit.com
            X509v3 Certificate Policies:
                Policy: 2.23.140.1.2.1
            CT Precertificate SCTs:
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log ID    : 48:B0:E3:6B:DA:A6:47:34:0F:E5:6A:0
2:FA:9D:30:EB:
                                1C:52:01:CB:56:DD:2C:81:D9:BB:BF:A
B:39:D8:84:73
                    Timestamp : Apr 17 02:08:32.799 2024 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256
                                30:45:02:21:00:92:13:53:65:39:F8:9
9:E4:F1:56:AF:
                                7E:AD:31:95:7A:DF:9D:71:8E:32:92:5
0:DC:4A:0B:76:
                                B1:64:FA:38:41:02:20:5C:77:44:2F:9
0:01:EE:4A:13:
                                D5:AF:43:57:BB:7A:9F:48:8A:4C:F0:A
6:E0:CE:66:66:
                                CE:46:F9:CF:3B:DB:9F
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log ID    : EE:CD:D0:64:D5:DB:1A:CE:C5:5C:B7:9
D:B4:CD:13:A2:
                                32:87:46:7C:BC:EC:DE:C3:51:48:59:4
6:71:1F:B5:9B
```

	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-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like: RewriteEngine on RewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P] ProxyPassReverse /here/ http://example.com:8080/ Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.
CVE-2022-37436	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

```
                    Timestamp : Apr 17 02:08:32.823 2024 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256
                                30:46:02:21:00:C7:44:CE:44:D3:4C:B
5:58:7D:8C:4F:
                                18:75:D3:68:E3:3B:95:CE:78:36:1A:8
1:77:A5:A9:94:
                                68:06:04:4B:93:02:21:00:FA:E5:37:7
2:DC:35:B6:77:
                                02:68:D6:E9:32:D8:9A:5C:6A:8F:ED:4
9:D4:A1:F0:67:
                                91:5F:72:8F:0C:4D:80:DF
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        90:d5:b3:67:e4:41:7a:8e:55:93:04:e4:c6:ee:67:11:ad:ca:
        a0:e9:5d:51:c4:30:90:55:85:e3:1a:32:e0:19:ce:9d:76:dc:
        82:9d:3e:74:bc:98:a3:5a:10:3e:f0:80:65:87:77:a6:d9:56:
        e0:a0:11:f9:25:56:fd:4a:c0:04:85:28:55:14:9a:6b:58:03:
        b0:59:7b:0f:7a:9c:68:54:88:6b:33:46:f1:a4:94:a5:fb:3d:
        86:b1:d6:0d:69:58:8c:63:e2:73:63:e1:7e:79:3b:8b:37:57:
        70:2a:9c:f4:92:2c:c4:57:95:3f:62:81:38:3e:8b:fd:71:ae:
        74:ef:bd:65:dc:86:f9:85:e6:b2:8e:17:24:5d:6c:6b:91:ca:
        fc:83:ca:64:e7:f8:de:62:e2:7e:bb:5a:52:ff:b0:71:0c:77:
        8c:b7:d3:dd:0d:94:87:8f:92:8d:69:53:b6:ec:d6:66:6b:fa:
        46:5d:63:d2:4f:20:fa:24:32:7c:0d:eb:6c:06:26:dc:6b:70:
        6c:d5:10:21:ff:9b:4a:1d:f3:f4:70:82:c3:eb:4b:54:80:8f:
        4a:51:96:81:5a:ab:98:5f:b9:b7:17:a1:54:c5:99:fc:aa:03:
        14:69:21:ef:27:d2:fd:bd:98:c4:ca:1f:b1:8f:5f:0a:8f:60:
        39:5b:87:36
```

	headers have any security purpose, they will not be interpreted by the client.
CVE-2022-36760	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 versions.
CVE-2022-31813	**7.5** 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-2022-30556	**5.0** 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-2022-29404	**5.0**	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-2022-28615	**6.4**	Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.
CVE-2022-28614	**5.0**	The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP

	Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.
CVE-2022-28330	**5.0** 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-2022-26377	**5.0** 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 2.4.53 and prior versions.
CVE-2022-23943	**7.5** 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-2022-22721	**5.8**	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-2022-22720	**7.5**	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-2022-22719	**5.0**	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-2013-4365	**7.5**	Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the

mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

CVE-2013-2765 **5.0** The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

CVE-2013-0942 **4.3** Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

CVE-2013-0941 **2.1** EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web

	Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.
CVE-2012-4360	**4.3** Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2012-4001	**5.0** The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to

		intranet servers.
CVE-2012-3526	5.0	The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.
CVE-2011-2688	7.5	SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.
CVE-2011-1176	4.3	The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by

	leveraging the root uid and root gid of an mpm-itk process.
CVE-2009-2299	**5.0** The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.
CVE-2009-0796	**2.6** Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.
CVE-2007-4723	**7.5** Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used,

	allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.
CVE-2006-20001	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.

// PRODUCTS

Monitor

Search Engine

Bulk Data

Images

// PRICING

Membership

API Subscriptions

// CONTACT US

support@shodan.io

Developer API

Snippets

Enterprise

Maps