192.31.2.6 sonar-west.net.yale.edu

City	New Haven
Country	United States
Organization	Yale University
ISP	Yale University
Last Update	2020-03-09T20:17:38.873499
Hostnames	sonar-west.net.yale.edu
ASN	AS29

Web Technologies

- D3
- DataTables
- Font Awesome
- Handlebars
- jQuery
- jQuery UI
- Modernizr
- Select2
- ZURB Foundation

Vulnerabilities

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

CVE-2011-5000	The ssh_gssapi_parse_ename function in gss-serv.c in OpenSSH 5.8 and earlier, when gssapi-with-mic authentication is enabled, allows remote authenticated users to cause a denial of service (memory consumption) via a large value in a certain length field. NOTE: there may be limited scenarios in which this issue is relevant.
CVE-2010-4478	OpenSSH 5.6 and earlier, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol, a related issue to CVE-2010-4252.
CVE-2014-1692	The hash_buffer function in schnorr.c in OpenSSH through

Ports

22 80 123 443 3001

Services

22
tcp
ssh

OpenSSH Version: 5.3

```
SSH-2.0-OpenSSH_5.3
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAABIwAAAQEA8bU+vhQyldEuockegUvByEglvwAxzWtF
5ladbRZfsyZ4sotF
5b4m5hqkzAABswSpuIGaFetSKHE8OtJTECSsQlY0SF3pSdbRJyVK8zdLc87goWx5J
rJf2a5NW8sF
EPCXOYqBbDfzGDcGYMlKf0nzX4DmBCEjGjdYjHvTZwK6C6DzR+MWbe+CyTDQZk/5s
gFFnm25tuGb
jLVb1yBMAVeJsW0b+20b4cmuzBzEthH2n/K9ZeCJTPzc8eao3GH7nZhEaRx6KG8ge
6W0/sSsuTYU
x0v0gm24khihPvHpbC0KWWshg4Dqyax40VNBC8V6wx/x2DQJxVT0LxJ1K+fvqNir7
Q==
Fingerprint: 2d:99:bf:87:e8:94:3d:af:54:84:d6:24:14:39:21:a2

Kex Algorithms:
 diffie-hellman-group-exchange-sha256
 diffie-hellman-group-exchange-sha1
 diffie-hellman-group14-sha1
 diffie-hellman-group1-sha1

Server Host Key Algorithms:
  ssh-rsa
  ssh-dss

Encryption Algorithms:
  aes128-ctr
  aes192-ctr
  aes256-ctr
  arcfour256
  arcfour128
  aes128-cbc
  3des-cbc
  blowfish-cbc
  cast128-cbc
  aes192-cbc
  aes256-cbc
  arcfour
 rijndael-cbc@lysator.liu.se

MAC Algorithms:
  hmac-md5
  hmac-sha1
```

	6.4, when Makefile.inc is modified to enable the J-PAKE protocol, does not initialize certain data structures, which might allow remote attackers to cause a denial of service (memory corruption) or have unspecified other impact via vectors that trigger an error condition.
CVE-2010-5107	The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.
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-2016-10708	sshd in OpenSSH before 7.4 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence NEWKEYS message, as demonstrated by Honggfuzz, related to kex.c and packet.c.
CVE-2016-0777	The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.
CVE-2011-4327	ssh-keysign.c in ssh-keysign in OpenSSH before 5.8p2 on certain platforms executes ssh-rand-helper with unintended open file descriptors, which allows local users to obtain sensitive key information via the ptrace system call.
CVE-2010-4755	The (1) remote_glob function in sftp-glob.c and the (2) process_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH_FXP_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.
CVE-2012-0814	The auth_parse_options function in auth-options.c in sshd in OpenSSH before 5.7 provides debug messages containing authorized_keys command options, which allows remote authenticated users to obtain potentially sensitive information by reading these messages, as demonstrated by the shared user account required by Gitolite. NOTE: this can cross privilege boundaries because a user account may intentionally have no shell or filesystem access, and therefore may have no supported way to read an authorized_keys file in its own home directory.

```
umac-64@openssh.com
hmac-sha2-256
hmac-sha2-512
hmac-ripemd160
hmac-ripemd160@openssh.com
hmac-sha1-96
hmac-md5-96

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

80
tcp
http

Apache httpd

```
HTTP/1.1 200 OK
Date: Tue, 03 Mar 2020 07:12:50 GMT
Server: Apache
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self' ; script-src 'self' '
unsafe-eval' 'unsafe-inline' ; img-src 'self' 'unsafe-inline' dat
a: ; style-src 'self' 'unsafe-inline' ; connect-src *
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8
```

123
udp
ntp

```
NTP
protocolversion: 3
stratum: 2
leap: 0
precision: -23
rootdelay: 0.00999450683594
rootdisp: 0.0234832763672
refid: 3330079834
reftime: 3792773718.59
poll: 3
```

443
tcp
https

Apache httpd

```
HTTP/1.1 200 OK
Date: Fri, 06 Mar 2020 13:49:53 GMT
Server: Apache
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self' ; script-src 'self' '
unsafe-eval' 'unsafe-inline' ; img-src 'self' 'unsafe-inline' dat
a: ; style-src 'self' 'unsafe-inline' ; connect-src *
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8
```

SSL Certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            6a:a2:d9:b5:c4:0a:dc:16:dd:11:b8:f8
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=BE, O=GlobalSign nv-sa, CN=GlobalSign Organizat
```

```
ion Validation CA - SHA256 - G2
        Validity
            Not Before: Apr  7 11:41:07 2017 GMT
            Not After : Apr  7 11:41:07 2020 GMT
        Subject: C=US, ST=Connecticut, L=New Haven, O=Yale Univer
sity, CN=sonar-west.net.yale.edu
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:c5:f4:26:e2:f4:f4:06:92:ad:e5:62:8a:21:cf:
                    a9:09:1f:ec:b4:9d:fb:6b:38:ba:79:b1:de:82:2f:
                    ef:25:2c:75:4b:db:ff:05:d0:a5:21:35:ba:2a:bb:
                    bd:8f:58:64:3b:7b:dd:48:17:98:3e:1c:e6:81:57:
                    25:26:3a:18:88:2b:db:82:55:20:a2:f1:62:e3:2f:
                    22:c4:92:a8:d6:36:05:b5:16:35:1d:ba:31:d7:51:
                    ed:34:85:7d:d5:92:06:77:0c:5d:35:cc:15:0d:81:
                    6c:ed:cb:78:7f:44:7f:c0:2e:2f:96:e4:b2:61:5b:
                    77:67:42:92:c5:7e:2c:6f:e6:e1:f3:d3:4b:b6:ca:
                    b0:e0:50:65:cc:d1:a9:27:f2:94:58:fc:4e:30:2a:
                    53:2d:25:e4:53:33:4b:87:66:9b:0d:45:92:df:40:
                    20:79:ae:1e:47:e1:56:a0:33:3e:d8:f4:f0:dd:26:
                    53:83:c9:e1:00:7b:a2:25:91:54:18:3e:c5:94:c0:
                    ab:c1:2f:0d:7c:fa:26:67:23:2a:5c:bb:e1:e3:54:
                    95:6d:53:d2:57:06:e2:3f:bc:0f:2e:99:48:e0:d0:
                    c0:4d:ea:62:4b:c5:00:a1:86:ae:70:0b:e6:08:3c:
                    51:b8:8e:94:d3:1e:d8:ec:d9:e2:6e:a9:f0:b0:de:
                    4c:24:85:5e:c7:d2:a2:56:53:bb:a0:09:d7:e7:f2:
                    92:e2:6f:94:08:81:b8:ad:03:03:ce:2e:13:01:f2:
                    72:5d:57:cd:c1:f6:4a:0a:a3:7f:26:cf:96:0d:0a:
                    04:a0:4f:6b:ca:30:6f:a1:62:5e:97:80:10:63:2b:
                    81:90:76:6e:5c:e3:ec:ef:cc:6a:d9:6a:a6:6a:5d:
                    ce:a8:73:90:25:6f:ea:8d:d0:1b:bf:96:c5:4d:e3:
                    21:12:37:2c:1c:6b:83:0f:a2:f3:24:88:41:70:64:
                    b2:8f:e7:e6:1f:85:b4:3f:e3:fd:91:06:4b:5c:e9:
                    93:6c:d3:e6:fc:43:6d:d3:ef:99:1a:c3:da:5c:ac:
                    ea:8e:86:7f:a3:e6:91:e0:ec:9c:5d:5b:17:a5:31:
                    e9:e3:b9:9e:74:c5:d2:f8:41:72:f1:08:03:35:40:
                    49:ba:fa:43:5a:bc:72:19:37:09:83:f6:13:81:bf:
                    07:c1:11:35:ac:ed:0b:b2:79:27:cf:a0:d6:c5:8a:
                    f3:f7:50:1d:dc:fb:7a:23:2c:0f:c8:4d:cb:79:c4:
                    f7:8c:57:b1:c4:00:68:6a:3a:dc:b1:05:40:e1:61:
                    9f:35:14:54:be:6f:b2:45:5c:2b:f7:d0:0a:c3:5b:
                    9f:5b:23:a4:d8:76:33:34:39:12:bd:57:2b:42:0d:
                    c5:5b:6b
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            Authority Information Access:
                CA Issuers - URI:http://secure.globalsign.com/cac
ert/gsorganizationvalsha2g2r1.crt
                OCSP - URI:http://ocsp2.globalsign.com/gsorganiza
tionvalsha2g2

            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.4146.1.20
                  CPS: https://www.globalsign.com/repository/
                Policy: 2.23.140.1.2.2

            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://crl.globalsign.com/gs/gsorganization
valsha2g2.crl

            X509v3 Subject Alternative Name:
                DNS:sonar-west.net.yale.edu
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Aut
hentication
            X509v3 Subject Key Identifier:
                32:4B:E9:B1:8F:D7:88:70:9F:3B:DE:75:39:B6:D9:51:1
6:80:EA:49
            X509v3 Authority Key Identifier:
                keyid:96:DE:61:F1:BD:1C:16:29:53:1C:C0:CC:7D:3B:8
3:00:40:E6:1A:7C
```

```
Signature Algorithm: sha256WithRSAEncryption
     83:65:d5:ac:ef:a3:b9:6e:83:7c:db:5d:69:3f:36:e6:10:2b:
     ed:46:46:fd:26:10:eb:69:af:75:a2:56:2b:1c:e2:98:63:24:
     2e:c2:98:e1:8c:d3:6a:e0:8d:a3:9a:6a:8f:01:c6:50:bc:43:
     32:98:9c:16:8c:73:d1:ac:e3:ab:34:71:47:5b:ff:af:81:27:
     d2:a7:55:14:9f:ca:da:5f:18:14:fe:bf:20:dd:c9:e7:83:3e:
     59:b1:37:0e:98:6f:5d:1e:f1:74:1a:91:64:a3:e9:48:4f:a7:
     23:39:e0:ca:ef:36:05:7f:3d:96:bc:59:ff:d8:11:88:33:59:
     cd:ca:06:eb:f6:bd:43:c8:dd:36:50:9b:62:ea:a5:86:31:5f:
     b3:51:d3:89:03:d7:7a:ae:f5:45:3d:aa:c2:19:b4:39:23:de:
     aa:72:bf:6b:c1:30:49:59:bf:78:a1:8a:0c:e6:c3:23:6b:43:
     64:53:c9:5c:b0:8b:c7:4e:bb:16:27:5a:4d:91:bc:a6:e3:a6:
     1f:9c:da:9f:ed:59:6b:99:01:bf:4a:5a:19:04:9b:96:ff:37:
     74:3e:36:76:2a:a1:25:74:a3:4e:b1:20:b3:80:79:a8:bc:22:
     64:77:fb:ec:2c:d3:e3:e2:3c:c6:68:7b:f6:08:e5:34:f6:88:
     8d:ad:6d:3a
```

3001
tcp
https-simple-new