140.247.116.37

City	Cambridge
Country	United States
Organization	Harvard University
ISP	Harvard University
Last Update	2020-03-09T22:53:16.517222
ASN	AS1742

Vulnerabilities

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

CVE-2019-6111	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). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).
CVE-2019-6110	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-2018-20685	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-2019-6109	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 affects refresh_progress_meter() in progressmeter.c.

Ports

22 88 3283 5900 8081

Services

22
tcp
ssh

OpenSSH Version: 7.9

```
SSH-2.0-OpenSSH_7.9
Key type: ssh-ed25519
Key: AAAAC3NzaC1lZDI1NTE5AAAAIDHm+Yn2KOq+UTxc8e9tczT4ZVGYeGdFSf82
b3HuWfI8
Fingerprint: 37:54:08:8a:60:72:72:e0:e8:63:f0:ec:83:03:fc:5a

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-group14-sha256
 diffie-hellman-group14-sha1

Server Host Key Algorithms:
 rsa-sha2-512
 rsa-sha2-256
 ssh-rsa
 ecdsa-sha2-nistp256
 ssh-ed25519

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
```

88
udp
kerberos

```
~b0`\xa0\x03\x02\x01\x05\xa1\x03\x02\x01\x1e\xa4\x11\x18\x0f20200
309122907Z\xa5\x05\x02\x03\x08f>\xa6\x03\x02\x01<\xa9\x04\x1b\x02
NM\xaa\x170\x15\xa0\x03\x02\x01\x00\xa1\x0e0\x0c\x1b\x06krbtgt\x1
b\x02NM\xab\x16\x1b\x14No client in request
```

3283
udp
ard

Apple Remote Desktop

```
Name: pol-f5kqm02mf694
```

5900
tcp
http-simple-new

Apple remote desktop vnc

```
RFB 003.889
```