**GeneralInformation**

|  |  |
| --- | --- |
| Hostnames | **abhayamshelter.com** cpanel.**abhayamshelter.com** cpcalendars.**abhayamshelter.com** cpcontacts.**abhayamshelter.com** mail.**abhayamshelter.com** webdisk.**abhayamshelter.com** webmail.**abhayamshelter.com** www.**abhayamshelter.com** in3.**fastwebhost.com** **mychoicesarees.com** cpanel.**mychoicesarees.com** cpcalendars.**mychoicesarees.com** cpcontacts.**mychoicesarees.com** mail.**mychoicesarees.com** webdisk.**mychoicesarees.com** webmail.**mychoicesarees.com** www.**mychoicesarees.com** |
| Domains | [ABHAYAMSHELTER.COM](https://www.shodan.io/domain/abhayamshelter.com) [FASTWEBHOST.COM](https://www.shodan.io/domain/fastwebhost.com) [MYCHOICESAREES.COM](https://www.shodan.io/domain/mychoicesarees.com) |
| Country | [United States](https://www.shodan.io/search?query=country%3A%22US%22) |
| City | [Los Angeles](https://www.shodan.io/search?query=city%3A%22Los+Angeles%22) |
| Organization | [ReliableSite.Net LLC](https://www.shodan.io/search?query=org%3A%22ReliableSite.Net+LLC%22) |
| ISP | [ReliableSite.Net LLC](https://www.shodan.io/search?query=isp%3A%22ReliableSite.Net+LLC%22) |

**Port number 2082**

**Vulnerabilities: -**

1.Bruteforce Attacks

2.Exploitation of software vulnerabilities

3.Denial of service

4.Misconfigurations

**Port number 2083**

**Vulnerabilities: -**

1.SSL/TLS vulnerabilities

2.Bruteforce

3.XSS

4.CSRF

5.DOS

**Port number 2086**

**Vulnerabilities: -**

1.Bruteforce

2.software exploits

3.DOS

4.Misconfigurations

**Vulnerabilities**

**CVE-2023-51385**

Business Impact: -

A critical vulnerability has been identified in SSH Proxy Command, marked as CVE-2023-51385, with a severity rating of 9.8 on the CVSS scale. This flaw poses a significant risk, potentially allowing attackers to execute arbitrary code through shell injection on vulnerable servers.

**CVE-2023-51384**

Business Impact: -

In ssh-agent in OpenSSH before 9.6, certain destination constraints can be incompletely applied. When destination constraints are specified during addition of PKCS#11-hosted private keys, these constraints are only applied to the first key, even if a PKCS#11 token returns multiple keys.

[**CVE-2023-48795**](https://www.shodan.io/search?query=vuln%3ACVE-2023-48795)

Business Impact: -

The most significant identified impact is that it enables a MITM to delete the SSH2\_MSG\_EXT\_INFO message sent before authentication begins. This allows the attacker to disable a subset of keystroke timing obfuscation features. However, there is no other observable impact on session secrecy or session integrity.

**CVE-2023-38408**

Business Impact: -

The Impact of OpenSSH Vulnerability CVE-2023-38408 Successful exploitation of this vulnerability allows a remote attacker to execute arbitrary commands on vulnerable OpenSSH forwarded ssh-agent. This poses a significant security risk, especially considering the widespread use of OpenSSH.

**CVE-2021-36368**

Business Impact: -

If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server.

**CVE-2020-15778**

Business Impact: -

The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. A flaw was found in the scp program shipped with the openssh-clients package.

**CVE-2019-6111**

Business Impact: -

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.

**CVE-2019-6110**

Business Impact: -

Description. The MITRE CVE dictionary describes this issue as: 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-2019-6109**

Business Impact: -

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.

**CVE-2018-20685**

Business Impact: -

The MITRE CVE dictionary describes this issue as: 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.