

Google Bard Vulnerability Fixes Result

Query:

Give me the short fixes for the vulnerability (CVE-2020-15778)

Result:

While there is no official patch for CVE-2020-15778, the OpenSSH project has recommended the following workarounds to mitigate the risk:

1. **Avoid using backtick (`) characters in file names:** This is the primary way that attackers can exploit the vulnerability. By avoiding backticks, you can significantly reduce your risk of exposure.
2. **Use scp with caution:** If you must use scp, be sure to use it only with trusted sources and be careful about the files you transfer.
3. **Upgrade to OpenSSH 8.4p1 or later:** This version of OpenSSH includes a fix for CVE-2020-15778. However, it is important to note that upgrading to a new version of OpenSSH may break compatibility with older systems.

In addition to these workarounds, you may also want to consider implementing the following security measures:

1. **Enable host-based authentication:** This will require users to authenticate themselves to the SSH server using their SSH keys, rather than their passwords. This can make it more difficult for attackers to gain access to your system.
2. **Use firewall rules to restrict access to SSH ports:** This will help to protect your system from unauthorized access.
3. **Keep your systems up to date:** This will help to ensure that you have the latest security patches installed.

By following these workarounds and security measures, you can help to protect your systems from CVE-2020-15778.

Query:

Give me the short fixes for the vulnerability (CVE-2020-15778)

Result:

Sure, here are the short fixes for the vulnerability (CVE-2020-15778):

Avoid using backtick (`) characters in file names. This is the primary way that attackers can exploit the vulnerability. By avoiding backticks, you can significantly reduce your risk of exposure.

Use scp with caution. If you must use scp, be sure to use it only with trusted sources and be careful about the files you transfer.

Upgrade to OpenSSH 8.4p1 or later. This version of OpenSSH includes a fix for CVE-2020-15778. However, it is important to note that upgrading to a new version of OpenSSH may break compatibility with older systems.

Query:

Give me the short fixes for the vulnerability (PRION:CVE-2020-12062)

Result:

CVE-2020-12062 is a vulnerability in the scp client in OpenSSH 8.2 that allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. This is because the scp client incorrectly sends duplicate responses to the server upon a utimes system call failure.

Here are some short fixes for the vulnerability:

- * Disable the `http_proxy` and `https_proxy` environment variables. This will prevent curl from using a proxy server, which can be exploited by attackers.
- * Use a trusted proxy server. If you must use a proxy server, make sure it is a trusted source and that you are aware of the risks involved.
- * Upgrade to curl 7.77.0 or later. This version of curl includes a fix for CVE-2020-12062.

Here are some additional recommendations to mitigate the risk of this vulnerability:

- * Use a strong password for your SSH user account.
- * Avoid using the `scp` command to transfer files to untrusted servers.
- * Use a secure file transfer protocol, such as SFTP or FTPS, to transfer files to untrusted servers.

Query:

Give me the short fixes for the vulnerability (PRION:CVE-2020-12062)

Result:

Sure, here are the short fixes for the vulnerability (CVE-2020-12062):

****Disable the `http_proxy` and `https_proxy` environment variables.**** This will prevent curl from using a proxy server, which can be exploited by attackers.

****Use a trusted proxy server.**** If you must use a proxy server, make sure it is a trusted source and that you are aware of the risks involved.

****Upgrade to curl 7.77.0 or later.**** This version of curl includes a fix for CVE-2020-12062.

****Upgrade to OpenSSH 8.2p1 or later.**** This version of OpenSSH includes a fix for CVE-2020-12062.

In addition to these short fixes, you can also help to protect your systems from CVE-2020-12062 by following these recommendations:

- * ****Use a strong password for your SSH user account.****
- * ****Avoid using the `scp` command to transfer files to untrusted servers.****

* **Use a secure file transfer protocol, such as SFTP or FTPS, to transfer files to untrusted servers.**

By following these fixes and recommendations, you can help to protect your systems from CVE-2020-12062.

Query:

Give me the short fixes for the vulnerability (PRION:CVE-2016-20012)

Result:

CVE-2016-20012 is a vulnerability in OpenSSH that allows remote attackers to test whether a certain combination of username and public key is known to an SSH server.

Here are some short fixes for the vulnerability:

* **Upgrade to OpenSSH 7.3 or later.** This version of OpenSSH includes a fix for CVE-2016-20012.

* **Disable the `pubkey_auth` option in the SSH server configuration file.** This will prevent the server from accepting public key authentication requests.

* **Use a strong password for your SSH user account.** This will make it more difficult for attackers to guess the username and public key combination.

* **Avoid using the same public key for multiple SSH user accounts.** This will make it more difficult for attackers to use a public key to gain access to multiple accounts.

Here are some additional recommendations to mitigate the risk of this vulnerability:

* **Use a firewall to block SSH connections from untrusted networks.**

* **Use a secure shell, such as SSH2, to encrypt SSH traffic.**

* **Monitor your SSH logs for suspicious activity.**

By following these fixes and recommendations, you can help to protect your systems from CVE-2016-20012.