Search blog

Blog Home

Cookiebot by Usercentrics

This website uses cookies

We use cookies, pixel tags, and other tracking technologies on our site to enhance site navigation, analyze site usage, and assist in our marketing efforts. With your consent, we may also share information about your website visit through these technologies with third parties for analytics and advertising purposes.

Show details

Allow all

Customize

Reject all

The Qualys Threat Research Unit (TRU) has discovered a remote code execution vulnerability in OpenSSH's forwarded ssh-agent. This vulnerability allows a remote attacker to potentially execute arbitrary commands on vulnerable OpenSSH's forwarded ssh-agent. Given the widespread use of OpenSSH's forwarded ssh-agent Qualys Research Unit recommends that security teams apply patches for this vulnerability on priority.

About OpenSSH's Agent Forwarding

The ssh-agent is a background program that caches private keys for SSH public key authentication, reducing the need for regular passphrase input. Initiated at the start of an X or login session, it operates by storing keys in memory and unloading only when the process ends.

It's instrumental in automation scripts or tasks requiring frequent server connections, as it prevents the need for insecure password storage or constant passphrase input. The connections to ssh-agent may be forwarded from further remote to avoid the need for authentication data to be stored on other machines. Nonetheless, it's still crucial to secure the keys with robust passphrases.

Cookiebot by Usercentrics

This website uses cookies

We use cookies, pixel tags, and other tracking technologies on our site to enhance site navigation, analyze site usage, and assist in our marketing efforts. With your consent, we may also share information about your website visit through these technologies with third parties for analytics and advertising purposes.

Show details ›

›

2023-07-06: Draft advisory and initial patch sent to OpenSSH.

2023-07-07: OpenSSH sent refined patches.

2023-07-09: Feedback on patches sent to OpenSSH.

2023-07-11: Received final patches from OpenSSH; feedback sent.

2023-07-14: OpenSSH plans for security-only release on July 19th.

2023-07-19: Coordinated release.

Technical Details

You can find the technical details of these vulnerabilities at:

https://www.qualys.com/2023/07/19/cve-2023-38408/rce-openssh-forwarded-ssh-agent.txt

https://www.qualys.com/2023/07/19/cve-2023-38408/rce-openssh-forwarded-ssh-

Cookiebot by Usercentrics

This website uses cookies

We use cookies, pixel tags, and other tracking technologies on our site to enhance site navigation, analyze site usage, and assist in our marketing efforts. With your consent, we may also share information about your website visit through these technologies with third parties for analytics and advertising purposes.

Show details

rigorous security measures and immediate response. Even robust systems can harbor hidden vulnerabilities, as demonstrated by the shortcomings of the ssh-agent. Proactively rectifying such vulnerabilities through actions such as implementing patches is critical to maintaining the integrity of digital assets.



Written by
Saeed Abbasi, Head of Threat Research Unit (TRU), Director of Product, Qualys
Write to Saeed at sabbasi@qualys.com

Share

Related content
vulnerabilities

Cookiebot by Usercentrics

This website uses cookies

We use cookies, pixel tags, and other tracking technologies on our site to enhance site navigation, analyze site usage, and assist in our marketing efforts. With your consent, we may also share information about your website visit through these technologies with third parties for analytics and advertising purposes.

Show details

Start a discussion

Follow us on

Cookiebot by Usercentrics

This website uses cookies

We use cookies, pixel tags, and other tracking technologies on our site to enhance site navigation, analyze site usage, and assist in our marketing efforts. With your consent, we may also share information about your website visit through these technologies with third parties for analytics and advertising purposes.

Show details ›

›