Loading...

[DECEMBER 18, 2023 · LEE PAINTER]

Important Java SSH Security Update: New SSH Vulnerability Discovered – CVE-2023-48795



Today, we bring to your attention a critical security announcement that demands immediate attention from system administrators, security professionals, and all Secure Shell (SSH) technology users. A team of security researchers from Ruhr University Bochum has uncovered significant vulnerabilities in SSH, which seriously threaten channel integrity. You can find comprehensive details of these findings at https://terrapin-attack.com.

Vulnerability Overview

The discovered vulnerabilities primarily involve two types of attacks:

1. **Prefix Truncation Attack on BPP**: This attack allows an intruder to manipulate sequence numbers during the SSH handshake, removing initial messages on the secure channel without triggering a MAC failure. The vulnerable cipher modes are ChaCha20-Poly1305 and Encrypt-then-MAC algorithms.

2. **Extension Negotiation Downgrade Attack**: This attack compromises channel security by removing extension info messages. It's particularly concerning because it affects all compliant SSH implementations, enabling attackers to bypass specific security extensions like the ping extension in OpenSSH 9.5.

Consequences and Exploits

With channel integrity compromised, several exploits, including severe ones against AsyncSSH due to additional implementation flaws, become possible. These vulnerabilities represent a significant risk, as they could allow unauthorized access and data manipulation.

Mitigations and Countermeasures

In response to these vulnerabilities, the researchers have worked closely with OpenSSH maintainers to develop a new protocol known as "strict kex". This protocol includes measures such as terminating connections upon receipt of unexpected or out-of-sequence packets and resetting packet sequence numbers at each SSH2_MSG_NEWKEYS message. An updated version of OpenSSH incorporating these countermeasures will be released concurrently with the public disclosure.

Turning off the affected cipher modes (chacha20-poly1305 and any encrypt-then-mac variants) is recommended as a less invasive alternative until the updates are applied. Other cipher modes, like AES-GCM, remain unaffected and can be used safely.

Public Disclosure and Resources

The vulnerability has been assigned the identifier CVE-2023-48795. Detailed findings, alongside an informational website for system administrators, have been published at https://terrapin-attack.com. We urge all relevant parties to prepare for this update and take necessary actions to secure their systems.

This announcement is a critical reminder of the ever-evolving landscape of cybersecurity threats and the need for constant vigilance and proactive measures. Stay tuned for further updates, and ensure your systems are ready for the necessary changes to maintain security and integrity.

This vulnerability has been fixed in the Java SSH Libraries and versions below.

Maverick Legacy Client
1.7.56

Maverick Legacy Server
1.7.56

Maverick Synergy Hotfixes
3.0.22

Maverick Synergy (Open Source)
3.1.0-SNAPSHOT

Post Views: 3,450

© 2026 Jadaptive Limited — Engineered in the open. Built with WordPress.