Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Terrapin Attack Downgrading the Fortresses of SSH

Date of Publication	Admiralty Code	TA Number
December 29, 2023	A1	TA2023525

Summary

First Seen: December 18, 2023
Affected Product: OpenSSH and its Implementation
Impact: The Terrapin attack, a cryptographic exploit targeting the widely adopted SSH protocol, poses a threat to the security of over 15 million servers dispersed across the Internet. This vulnerability enables attackers to compromise the security of established connections by truncating the extension negotiation message.

CVEs

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	PATCH
CVE-2023-48795	OpenSSH Terrapin Attack	OpenSSH	✗	✗	✓
CVE-2023-46445	AsyncSSH Rogue Extension Negotiation	AsyncSSH	✗	✗	✓
CVE-2023-46446	AsyncSSH Rogue Session Attack	AsyncSSH	✗	✗	✓

Vulnerability Details

#1 The Terrapin attack is a cryptographic exploit that targets the widely adopted SSH protocol, a crucial component for ensuring secure command-and-control across the expanse of the Internet. This sophisticated offensive maneuver compromises the security of SSH through the adept execution of an attack facilitated by man-in-the-middle interception.

#2 Notably documented under CVE-2023-48795, the Terrapin attack extends its reach by exploiting two additional vulnerabilities discovered in AsyncSSH, meriting the designations CVE-2023-46445 and CVE-2023-46446. Terrapin orchestrates the manipulation of sequence numbers during the handshake phase, thereby undermining the integrity of the SSH channel, especially when specific encryption modes like ChaCha20-Poly1305 or CBC with Encrypt-then-MAC are employed.

#3 The attack method employs prefix truncation attacks, involving the strategic injection and deletion of messages during the negotiation of features. Furthermore, it deftly manipulates sequence numbers in a manner that induces the disregarding of other messages, all while avoiding the detection of errors by both the client and server.

#4 SSH, an omnipresent internet standard, facilitates secure access to over 15 million servers dispersed across the open internet and various network services. Its functionalities encompass critical operations, including file transfers and remote terminal logins within corporate networks. The manipulative tactics employed by Terrapin empower attackers to tamper with or remove messages exchanged through the communication channel, ultimately leading to the downgrading of public key algorithms integral to user authentication.

#5 Additionally, this manipulation disables defenses against keystroke timing attacks in OpenSSH 9.5, deployed across approximately 56,204 publicly accessible servers. While the architects of SSH have implemented a remedy for the Terrapin attack, its efficacy is contingent upon the comprehensive upgrade of both client and server implementations to accommodate the fix.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-48795	OpenSSH 9.0 to 9.5	cpe:2.3:a:openbsd:openssh:*:*:*:*:*:*:*:*	CWE-354
CVE-2023-46445	AsyncSSH 2.0 to 2.14	cpe:2.3:a:asyncssh_project:asyncssh:*:*:*:*:*:*:*:*	CWE-345
CVE-2023-46446			CWE-639

Recommendations

Apply Official Fixes Immediately: Users affected by this issue are advised to promptly consult the vendor advisories for impacted implementations, applications, and Linux distributions. This includes **AsyncSSH**, **LibSSH**, **OpenSSH**, **PuTTY**, **Transmit**, **SUSE**, and others. Install the provided fixes and patches according to the respective vendor guidelines for enhanced security.

Update Win32-OpenSSH Implementation: We recommend that users of Win32-OpenSSH, the SSH implementation integrated into Windows 10, 11, Server 2019, and 2022, manually update their implementations to version 9.5.0.0p1-Beta.

Terrapin Scanner: Consider using a simple console application coded in Go to evaluate the vulnerability of your SSH server or client to the Terrapin attack. The **scanner** can connect to your SSH server, identify vulnerable encryption modes, and verify support for the strict key exchange countermeasure.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0007 Discovery	TA0011 Command and Control	T1190 Exploit Public-Facing Application	T1059 Command and Scripting Interpreter
T1565 Data Manipulation	T1565.002 Transmitted Data Manipulation	T1040 Network Sniffing	T1557 Adversary-in-the-Middle
T1600 Weaken Encryption	T1071 Application Layer Protocol		

Patch Details

To access details about patches, users affected by this flaw are encouraged to refer to vendor release notes on impacted implementations, applications, and Linux distributions. This encompasses platforms like AsyncSSH, LibSSH, OpenSSH, PuTTY, Transmit, SUSE, and other pertinent implementations.

Links:
https://terrapin-attack.com/patches.html
https://asyncssh.readthedocs.io/en/latest/changes.html#release-2-14-2-18-dec-2023
https://www.libssh.org/2023/12/18/libssh-0-10-6-and-libssh-0-9-8-security-releases/
https://www.openssh.com/releasenotes.html
https://www.chiark.greenend.org.uk/~sgtatham/putty/wishlist/vuln-terrapin.html
https://help.panic.com/releasenotes/transmit5/
https://www.suse.com/c/suse-addresses-the-ssh-v2-protocol-terrapin-attack-aka-cve-2023-48795/

References

https://terrapin-attack.com/

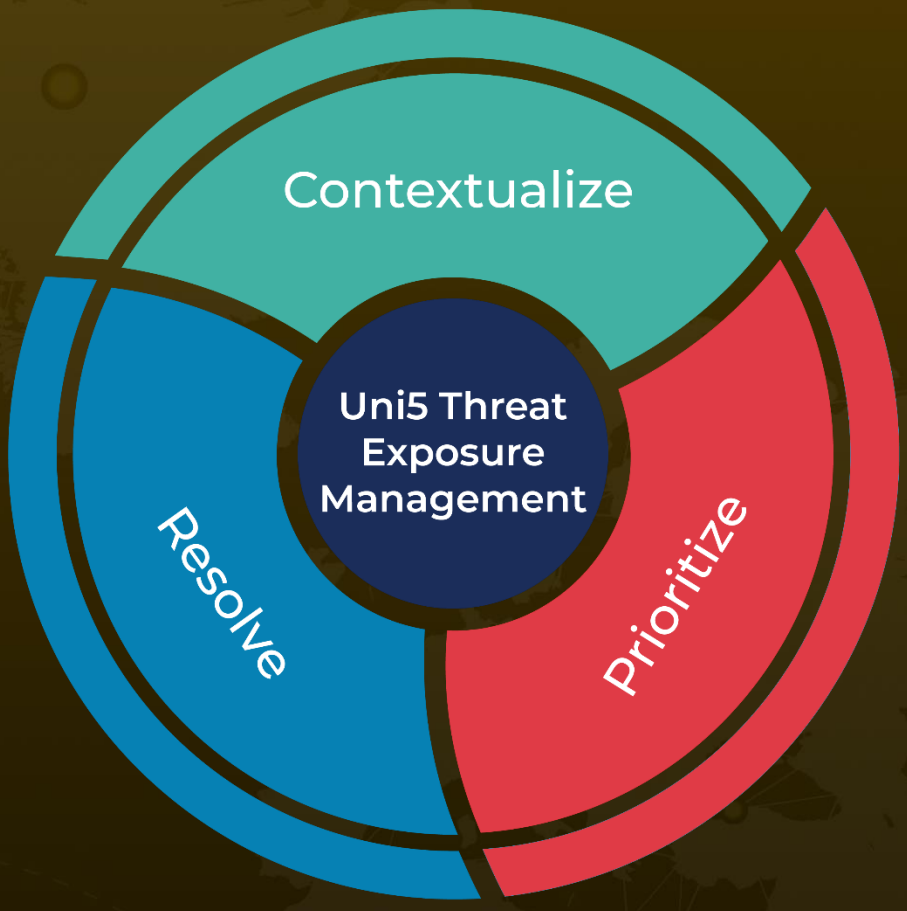
https://threatprotect.qualys.com/2023/12/22/ssh-vulnerability-used-in-terrapin-attacks-cve-2023-48795/

https://www.helpnetsecurity.com/2023/12/19/ssh-vulnerability-cve-2023-48795/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

December 29, 2023 . 1:00 AM

More at www.hivepro.com