Bug 920280 (CVE-2023-48795) - [Tracker] Terrapin Vulnerability

Status: CONFIRMED
Alias: CVE-2023-48795
Product: Gentoo Security
Component: Vulnerabilities (show other bugs)
Hardware: All Linux
Importance: Normal normal
Assignee: Gentoo Security
URL: https://terrapin-attack.com/
Whiteboard:
Keywords: Tracker
Depends on: 920293 920299 920421 920682 ~~920291~~ ~~920292~~ ~~920304~~ ~~920385~~ ~~921290~~ ~~930152~~
Blocks:
Show dependency tree

Reported: 2023-12-18 17:03 UTC by Christopher Fore
Modified: 2024-04-20 16:47 UTC (History)
CC List: 4 users (show)
See Also:

Attachments
Add an attachment (proposed patch, testcase, etc.)

Note
You need to log in before you can comment on or make changes to this bug.

Note: Please do not mark this bug as resolved after bumping or stabilizing. The Security Team will take care of that. Thanks.

Christopher Fore Dev Sec **2023-12-18 17:03:28 UTC** Description

```
CVE-2023-48795 (https://terrapin-attack.com/):

The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before
9.6 and other products, allows remote attackers to bypass integrity checks such
that some packets are omitted (from the extension negotiation message), and a
client and server may consequently end up with a connection for which some security
features have been downgraded or disabled, aka a Terrapin attack. This occurs
because the SSH Binary Packet Protocol (BPP), implemented by these extensions,
mishandles the handshake phase and mishandles use of sequence numbers. For example,
there is an effective attack against ChaCha20-Poly1305 (and CBC with Encrypt-then-
MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -
etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API
before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP,
and PuTTY before 0.80; and there could be effects on Bitvise SSH through 9.31,
AsyncSSH through 2.14.1, libssh through 0.10.5, and golang.org/x/crypto through
2023-12-17.
```

David Sardari **2023-12-18 19:13:13 UTC** Comment 1

I've used the following command to mitigate on the client side:

sed -i "1i Ciphers -$(ssh -Q cipher | grep -e chacha20-poly1305@openssh.com -e -cbc | paste -d, -s -)" ~/.ssh/config

In my case, the following line got added before the first line of the file:

Ciphers -3des-cbc,aes128-cbc,aes192-cbc,aes256-cbc,chacha20-poly1305@openssh.com

Hanno Böck Dev **2023-12-19 07:40:07 UTC** Comment 2

CVE-2023-46445 and CVE-2023-46446 are issues in AsyncSSH, which Gentoo has not packaged, so I believe they are irellevant here.

Only CVE-2023-48795 refers to the Terrapin vulnerability in the SSH protocol itself that affects pretty much every SSH implementation.

Andreas Sturmlechner Dev **2024-04-20 13:12:58 UTC** Comment 3

Why was kde proj CCed here at all?

Christopher Fore Dev Sec **2024-04-20 16:47:53 UTC** Comment 4

(In reply to Andreas Sturmlechner from comment #3)
> Why was kde proj CCed here at all?

Looks it it might have carried over from this bug:
https://bugs.gentoo.org/920291