Security Advisory for **SSH zero Day CVE 2024-6387**

Utimaco has been made aware of a vulnerability affecting distribution of OpenSSH: This document provides an overview of the vulnerability, affected products and provides mitigation scenarios.

1 Affected products

- CSLAN 64bit 5.8c.0 (Operating system of the LAN appliance for Utimaco GP-HSM Se Series (u.Trust Anchor) are affected
- CSLAN 32bit version 5.3 (Operating system of the LAN appliance for Utimaco GP-HSM SE-Series (CryptoServer Segen2 and CSe) are not affected

2 Issue

2.1 Description

A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead to sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period.

This issue has been reserved in the Common Vulnerabilities and Exposures list as CVE-2024-6387.

Details can be found here: https://nvd.nist.gov/vuln/detail/CVE-2024-6387.

2.2 Detailed description

- OpenSSH versions earlier than 4.4p1

Security Advisory for **SSH zero Day CVE 2024-6387**

- OpenSSH versions between 8.5p1 and 9.8p1 (excluding)

The vulnerability is exploitable on glibc-based Linux distributions (e.g., Debian-based). As of July 1st, 2024, no exploitation has been identified in the wild, with proven exploitation occurring only under lab conditions on 32-bit Linux/glibc systems (with ASLR). Exploitation on 64-bit systems has not been proven but is believed possible.

Utimaco CSLAN 32-bit: is not affected by this vulnerability since it uses OpenSSH 7.6p1.

Utimaco CSLAN 64-bit: Is affected by this vulnerability, however, as described, exploitation on 64bit system has not been proven but is believed possible.

3 What To Do

3.1 Mitigation

A temporary workaround is to set LoginGraceTime to 0 in the OpenSSH configuration file. This will prevent unauthenticated sessions from being kept open but can lead to a denial of service if all connection slots are used. If you need more information or guidance, please contact our Technical Support.

4 Final fix and upcoming changes in next releases

Utimaco will include the patch on further release of its 64-bit CSLAN version.

Security Advisory for **SSH zero Day CVE 2024-6387**

5 Technical support

You can find technical support for Utimaco products in any of these ways:

- Download product information from https://support.hsm.utimaco.com/support
- Contact us at support@utimaco.com
- Contact our support hotline: EMEA +49 800-627-3081, Americas +1-844-UTIMACO (+1 844-884-6226), APAC +81 800-919-1301.

6 Legal notices

This Advisory is subject to the effective agreement executed between you and Utimaco IS GmbH, or otherwise the General Terms and Conditions of Utimaco IS GmbH: https://hsm.utimaco.com/terms-and-conditions/