Alcatel·Lucent Enterprise

Alcatel-Lucent Security Advisory No. SA-N0115 Ed. 01

OpenSSL X.509 Email Address Buffer Overflow Vulnerability

Summary

OpenSSL has released security advisories CVE-2022-3602 and CVE-2022-3786 regarding buffer overflow vulnerabilities in OpenSSL versions 3.0.0 to 3.0.6.

Description of the Vulnerability

A buffer overrun can be triggered in the OpenSSL X.509 certificate verification, specifically in name constraint checking. An attacker can craft a malicious email address to overflow four attacker-controlled bytes on the stack. This buffer overflow could result in a crash (causing a denial of service) or potentially remote code execution.

In a TLS client, this can be triggered by connecting to a malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects.

OpenSSL versions 3.0.0 to 3.0.6 are vulnerable to this issue.

Additional details on the vulnerability can be found at https://www.openssl.org/news/secadv/20221101.txt

Status on Alcatel-Lucent Enterprise Products

The ALE products that are impacted by the vulnerabilities are identified below.

Product Name	Release
OmniSwitch OS6360, OS6560, OS6465, OS6860/E/N, OS6865, OS6900, OS9900	AOS 8.9.R01 GA

The ALE products that are not impacted are identified below

Product Name	Release
OmniSwitch OS6360, OS6560, OS6465, OS6860/E/N, OS6865, OS6900, OS9900	AOS 8.8.R02 or earlier
OmniSwitch OS6250, OS6350, OS6450	All
OmniSwitch OS2260, OS2360	All
OmniAccess Stellar OAW-AP1101, OAW-AP12xx, OAW-AP13xx, OAW-AP14xx	All
OmniVista 2500	All
OmniVista Cirrus	All
OmniAccess WLAN Access Points	All
OmniAccess WLAN Controllers	All
OmniVista 3600	All

Workarounds

The OmniSwitch uses OpenSSL to secure communications that are used to manage the operation of the switch. The recommended best practice is that the interfaces on the switch used for this management traffic should be protected with network access restricted to authorized network administrators and authorized management related applications. This will reduce the likelihood that the operation of the OmniSwitch can be compromised.

Resolution for Alcatel-Lucent Enterprise affected products

To address this vulnerability, the OpenSSL module in AOS 8.9.R01 will be updated to version 3.0.7.

Information on software versions to address the vulnerabilities is provided below.

Product	Fixed in	Date
OmniSwitch OS6360, OS6560, OS6465, OS6860/E/N, OS6865, OS6900, OS9900	AOS 8.9.R1 patch	Target release is November 30, 2022

History

Ed.01 (2022 November 04): creation