Alcatel·Lucent Enterprise

Alcatel-Lucent Security Advisory No. SA-G0002 Ed. 01

General information about VxWorks Urgent 11

Summary

Vulnerability summary.

A vulnerability has been discovered in in the TCP/IP stack (IPnet), a component of certain versions of VxWorks. VxWorks is the operating system used in some ALE products. Specifically, VxWorks is used in OmniSwitch products using AOS 6.x software and in IP phone products using PhonexChange 2.x/3.x software.

References

- CVE-2019-12256 (V7NET-2423)
- CVE-2019-12257 (VXW6-87101)
- CVE-2019-12255 (VXW6-87100)
- CVE-2019-12260 (V7NET-2425)
- CVE-2019-12261 (V7NET-2425)
- CVE-2019-12263 (V7NET-2425)
- CVE-2019-12258 (V7NET-2426)
- CVE-2019-12259 (V7NET-2428)
- CVE-2019-12262 (V7NET-2427)
- CVE-2019-12264 (V7NET-2428)
- CVE-2019-12265 (V7NET-2428)

Description of the vulnerability and impacts

Please refer to the ARMIS blog post https://armis.com/urgent11/ and the official Windriver notice for detailed information https://www.windriver.com/security/announcements/tcp-ip-network-stack-ipnet-urgent11/

Status on Alcatel-Lucent Enterprise products

After analysis of the reported vulnerabilities, **no Alcatel-Lucent Enterprise products** are impacted by these vulnerabilities.

This status includes

- all IP phones using PhonexChange 2.x/3.x,
- all OmniSwitches using AOS 6.x.

Resolution for Alcatel-Lucent Enterprise affected products

No impact, no patch required

History

Ed.01 (2019 August 1st): advisory creation