Alcatel·Lucent Enterprise

Alcatel-Lucent Security Advisory No. SA-C0065 Ed. 01
OmniVista 8770 Remote Code Execution

Summary

Vulnerability publication has been made public about OmniVista 4760 and OmniVista 8770. It impacts Web Directory Consultation client and provides a potential remote code execution vulnerability to the system with high privileges.

References

Date: December 09th, 2019
Risk: High
Impact: Remote access / Disrupt service (denial of service)
Attack expertise: Skilled
Attack requirements: Remote (no account) on the same network plane as the product

External resources:

- Original blogpost: https://git.lsd.cat/g/omnivista-rce/src/master/README.md
- https://www.exploit-db.com/exploits/47761
- https://packetstormsecurity.com/files/155595/Alcatel-Lucent-Omnivista-8770-Remote-Code-Execution.html

Description of the vulnerability

The vulnerability is due to possible remote access to some session files used by WebDirectory consultation client. A full description of the discovery has been made public on the following post https://git.lsd.cat/g/omnivista-rce/src/master/README.md

Status on Alcatel-Lucent Enterprise products

Since OmniVista 4760 product is deprecated and there is no remaining support for several years, we won't develop any comment on this and we recommend upgrading to the latest version of OmniVista 8770.

List of products and releases concerned (or affected)

Product Name	Release
OmniVista 8770	Before 4.1.12

List of products and releases **NOT** concerned (or affected)

Product Name	Release
OmniVista 8770	4.2

Resolution for Alcatel-Lucent Enterprise affected products

Fixed Software Versions/Patches

Product	Fixed in	Date
OmniVista 8770	4.1.12	January week 5 of 2020
OmniVista 8770	4.2	April 2020 offer release

History

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