ALE Security Advisory	No. SA-C0071	Ed. 01

CVE-2024-29149 & CVE-2024-29150

Summary

Vulnerabilities have been discovered in embedded firmware of ALE phone sets equipped with USB Port.

References

Reference	CVE-2024-29149 & CVE-2024-29150
Date	06 May 2024
Risk	High
Impact	*See comments*
Attack expertise	High
Attack requirements	Access to USB port
CVSS score	7.3
Affected versions	ALE-300/400/500 NOE & SIP, ALE-20/h, ALE-30/h, Noe-3G EE: 80x8s – 8088
Fixed version	*See text below*

Description of the vulnerability

. CVE-2024-29149
This vulnerability allows a bad actor to load a non-ALE firmware, potentially modified, and bypass authentication of the firmware, allowing it to be installed.

CVE-2024-29150
This vulnerability can elevate privileges of an already logged admin up to root level. There is no expected negative effect to users.

Impacts

. CVE-2024-29149 : potential impacts can be leak of information, DDoS by installing malicious agent within the firmware.
CVE-2024-29150 : potential impact is access to non-authorized information within firmware. There is no impact to user as information accessed are only technical.

Special note

ALE strongly recommend all partners to upgrade firmware to latest available to avoid any misuse of those vulnerabilities. Normal upgrade process applies (both for OmniPCX Enterprise, OXO Connect, OXO Connect Evolution.
ALE has delivered all necessary firmware, and full OXO software for all supported versions.
For end customers, please refer to your business partner for actions to be made.

Resolution for Alcatel-Lucent Enterprise affected products.

The two vulnerabilities are fixed in the latest firmwares available on the business portal, for each affected terminal or range of terminals (access to firmwares is limited to Business Partners having a valid account) :

ALE Enterprise 300/400/500

- R210 NOE version 1.30.33.3264 => https://myportal.al-enterprise.com/a4F5I000000cTdvUAE
- R300 NOE version 1.40.22.4272 => https://myportal.al-enterprise.com/a4FSZ0000031vxU2AQ
- R310 NOE version 1.50.07.5140 => https://myportal.al-enterprise.com/a4FSZ00000APTTH2A5
- R310 SIP version 1.10.07.1142 => https://myportal.al-enterprise.com/a4FSZ00000APOuz2AH

ALE Essential 20/30/30H

- R300 TDM version 1.40.32 → 84x9_TDM-R300.1.40.32.4200 => https://myportal.al-enterprise.com/a4F5I000000UPXoUAO
- R300 IP version 1.40.32 → 84xx_NOE-R300.1.40.32.4200 => https://myportal.al-enterprise.com/a4F5I000000UPXtUAO
- R200 TDM version 1.20.51 → 84x9_TDM-R200.1.20.51.2374 => https://myportal.al-enterprise.com/a4F5I000000UPt1UAG
- R200 IP version 1.20.51 → 84xx_NOE-R200.1.20.51.2374 => https://myportal.al-enterprise.com/a4F5I000000UPswUAG
- R310 TDM version 1.50.08 → 84x9_TDM-R310.1.50.08.5136 => https://myportal.al-enterprise.com/a4FSZ00000APZF92AP
- R310 IP version 1.50.08 → 84xx_NOE-R310.1.50.08.5136 => https://myportal.al-enterprise.com/a4FSZ00000APUc02AH

80x8S

- R510 NOE version 5.45.97 → 80x8s_NOE-R510.5.45.97.4947 => https://myportal.al-enterprise.com/a4F5I00000092etUAA

8008/800G

- R510 NOE version 5.45.97 →8008_NOE-R510.5.45.97.4947 => https://myportal.al-enterprise.com/a4F5I00000092eoUAA

8018

- R510 NOE version 5.45.97 → 8018_NOE-R510.5.45.97.4947 => https://myportal.al-enterprise.com/a4F5I00000092epUAA

8088

- SIP (including huddle room mode) → R304.03.016.1.2549 => https://myportal.al-enterprise.com/a4F5I000000YSv4UAG

ALE-2/ALE-3

- R200 version 2.12.63 à ALE-3-SIP-R200_2.12.63.000.2528 => https://myportal.al-enterprise.com/a4F5I000000UPUQUA4

For OXO Connect, please access to regular URL.

History

01	06 May 2024	creation
02		