ALE Security Advisory No. SA-C0059 Ed. 01

OmniPCX Office remote control vulnerability - additional critical security recommendation for fighting fraud

Summary

This Security advisory provides important security recommendations for OmniPCX Office Rich Communication Edition and OXO Connect products to prevent unauthenticated remote person executing arbitrary command and eventually take control of a vulnerable system.

References

Risk: Critical
Impact: Take control, Confidentiality, Denial of Service, Leverage
Attack expertise: Skilled
Attack requirements: Remote (no account)
CVSS score: Base 9.8 (Critical), Temporal 8.5 (High), Environmental 8.5 (High)
CVSS vector:
3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/CR:H/IR:M/AR:M/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:H/MI:H/MA:H

Description of the security recommendation

Unauthenticated remote person executing arbitrary command and eventually taking control of an OmniPCX Office Rich Communication Edition or OXO Connect system or perform harmful actions.

This is due to an undetailed flaw in the device management functions of the product. It allows an unauthenticated remote attacker to run arbitrary code as a privileged user on the operating system of the product.

Status on Alcatel-Lucent Enterprise products

List of products and releases concerned (or affected)

Product Name	Release
OmniPCX Office Rich Communication Edition	Releases 10.x prior to R10.3 / 039.001
OXO Connect	Releases 2.x prior to R2.0 / 038.001 and R2.1 / 024.003

Mitigation

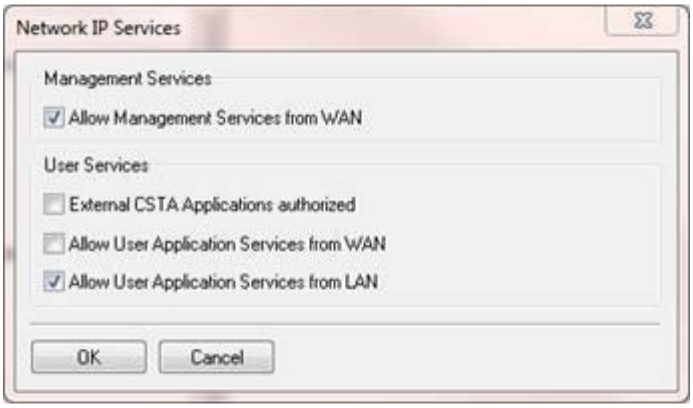
Software corrections are available on ALE business portal weblinks provided in “Fixed Software” section below. Otherwise, mitigation is possible by disabling services that can be a vector for the attack. Because this mitigation will restrict access and use of such services, it should be implemented with the end user’s concurrence.

For OXO RCE R10.0 and R10.1: Noteworthy address “ExtLnkClsd” disables all HTTP accesses to the system whether on LAN or WAN port except for system administration applications.

For OXO RCE R10.2, R10.3 and OXO Connect R2.0, R2.1: HTTP access to the system can be disabled for end user applications selectively on LAN and WAN. Two options are then possible:

1. Disabling “User application services from WAN” and restricting it to access from LAN only, prevents the system to be accessible from the Internet and thus limit the exposition to hackers.
2. Disabling both “User application services from WAN” and “User application services from LAN” so that the impacted services are disabled. As a consequence the vulnerability is no more exploitable by hackers.

Within an "OMC Installer" session: go to "System Miscellaneous"->"Network IP services"



Network IP Services

Management Services

☑ Allow Management Services from WAN

User Services

□ External CSTA Applications authorized

□ Allow User Application Services from WAN

☑ Allow User Application Services from LAN

The list of possible restricted services includes:

- MyIC 80x2 phones
- OTCV applications (all platforms)
- PIMphony, PIMphony Touch, MyIC Web Office
- IPDECT Lite
- SIP 8001 phone
- OT4135 phone
- WIFI AP1101

Since it leads to service restrictions for the end users, these workarounds must be considered as temporary mitigation actions only, pending installation of the above mentioned patch.

Additional security installation measures and recommendation can be found in the Technical Communication TC1143 available at https://businessportal2.alcatel-lucent.com/TC1143en

Fixed Software

Fixed Software Versions/Patches

Product	Fixed in	Date
OmniPCX Office Rich Communication Edition	OXO R10.3 / 039.001 https://businessportal2.alcatel-lucent.com/node/423311	June 16th, 2017
OXO Connect	OXO Connect R2.0 / 038.001 https://businessportal2.alcatel-lucent.com/node/432346	June 16th, 2017
OXO Connect	OXO Connect R2.1 / 024.003 https://businessportal2.alcatel-lucent.com/node/441226	June 16th, 2017

Exploitation and Public Announcements

ALE Product Security Incident Response Team (PSIRT) is to date not aware of any public announcement of malicious use that is described in this advisory note.

History

Ed.01 (2017 June 16th): document creation and publication