Alcatel-Lucent Security Advisory No. SA-C0068 Ed. 02 - CVE-2021-44228

Summary

A vulnerability has been discovered in Apache Log4j2 JNDI features used in configuration, log messages, and parameters that do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled.

References

Reference: CVE-2021-44228
Date: Dec10th, 2021
Risk: High
Impact: Execute arbitrary code
Attack expertise: Skilled
Attack requirements: Remote
CVSS score: 10.0 (critical)
Affected versions : >=2.0-beta9 and <=2.14.1
Fixed version: 2.15.0

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228

Description of the vulnerability

The vulnerability allows an attacker to inject arbitrary code in a payload to ask Log4J get access to data coming from a 3rd party. As Log4J do not check imported data for any non-allowed content (like commands), it allows the attack to be ran.

Impacts

Depending on the 3rd party service invoked, the impact may differ.

Status on Alcatel-Lucent Enterprise Communication products

List of products and releases

Product	*Versions*	*Affected*	*Impact*	*Remediation*
OmniPCX Enterprise	All	No	N/A	N/A
OmniPCX Office	All	No	N/A	N/A
OmniVista 8770	All	No	N/A	N/A
Cloud Connect	All	No	N/A	N/A
OpenTouch	All	Yes	*	Hotfix (1)
VAA	All	No	N/A	N/A
VNA	All	Yes	*	Upgrade (2)
O2G	All	No	N/A	N/A
EDS/EPS/Pegasus	All	No	N/A	N/A
OTEC (8770)	All	No	N/A	N/A
OTSBC	All	No	N/A	N/A
CCivr/CCS/CCA	All	No	N/A	N/A
Fax Server	*	*	*	*
ENS	All	No	N/A	N/A
IQ Messenger	All	No	N/A	N/A
OTNS	*	*	*	*
Soft panel Manager	All	No	N/A	N/A
OmniPCX Record	All	No	N/A	N/A
IPDSP	All	No	N/A	N/A
ManageMyPhone	All	No	N/A	N/A
SelfCare	All	No	N/A	N/A
CMMI	All	No	N/A	N/A
MGS	All	No	N/A	N/A
SGA	All	No	N/A	N/A
AVBS	All	No	N/A	N/A
CLickToConnect	All	No	N/A	N/A
Calendar	All	No	N/A	N/A
Dispatch Console	All	Yes	*	*

** : analysis ongoing*

Status on Alcatel-Lucent Enterprise Network products

List of products and releases

Product	Version	Affected	Impact	Remediation
PALM	Cloud	No	N/A	N/A
Subscription Manager	Cloud	No	N/A	N/A
Agnostic Data Lake	Cloud	No	N/A	N/A
Asset Tracking	Cloud	*	*	*
OV Cirrus	10.1	*	*	*
OV Cirrus	4.6R1 or earlier	*	*	*
OV 2500	4.6R1 or earlier	*	*	*
Ucopia	All	No	N/A	N/A
Clearpass	All	*	*	*
OV3600	All	*	*	*
LBS	Cloud	*	*	*
RAP Appliance	All	*	*	*
NaaS	Cloud	*	*	*
Titan SD-WAN	Cloud	No	N/A	N/A
OmniSwitch	All	No	N/A	N/A
Stellar AP	All	No	N/A	N/A

** : analysis ongoing*

Product	Version	Affected	Impact	Remediation
Aruba product line	See : http://www.arubanetworks.com/support-services/security-bulletins/.			

Status on Alcatel-Lucent Enterprise Cloud products

List of products and releases

Product	Version	Affected	Impact	Remediation
Rainbow UCaaS/CPaaS/Edge/HDS/Hub	All	No	N/A	N/A

Temporary remediation for Alcatel-Lucent Enterprise affected products

To confirm depending on affected products

Resolution for Alcatel-Lucent Enterprise affected products

(1) OpenTouch Solutions

- Hotfix by eW51 on OT 2.6.1 , OT 2.6 MD4,
- Hotfix for OT 2.5 MD6, OT2.5MD3 , OT2.4MD4 : Hotfix delivery date to be communicated on Dec 17
- Hotfix for OT 2.3.1 , OT2.2.1 : HF Feasibility under R&D analyze
- For customers using other versions , they have to update to the last MD of their release or to upgrade to a supported version to get a hotfix solving this vulnerability.

(2) VNA

- Upgraded version to be delivered the 17th of Dec' 2021

History

Ed.01 (2021 December 13th): creation

Ed.02 (2021 December 13th): Update on CBD solutions, add of NBD and CCBD solutions