



# Alcatel-Lucent Security Advisory No. SA-C0068 Ed. 05

## - 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 :  $\geq 2.0\text{-beta9}$  and  $\leq 2.14.1$

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 3<sup>rd</sup> 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 3<sup>rd</sup> party service invoked, the impact may differ.

### Special note

Although this Security Advisory has been triggered by initial CVE-2021-44228, the following status cover, in terms of risk, impact and action recommended by ALE, the CVE-2021-44228 and the CVE-2021-45046.

## Status on Alcatel-Lucent Enterprise Communication products

List of products and releases

Product	Versions	Affected	Impact	Remediation
<b>OmniPCX Enterprise</b>	All	No	N/A	N/A
<b>OmniPCX Office/ OXO Connect/ OXO Connect Evolution</b>	All	No	N/A	N/A
<b>OMC / PIMPhony/AST/Labset</b>	All	No	N/A	N/A
<b>OmniVista 8770</b>	All	No	N/A	N/A
<b>Cloud Connect</b>	All	No	N/A	N/A
<b>OpenTouch</b>	All	Yes	*	Hotfix (1)
<b>GAS Server (WebRTCGW,OMS, OS)</b>	All	No	N/A	N/A
<b>VAA</b>	All	No	N/A	N/A
<b>VNA</b>	All	Yes	*	Upgrade (2)
<b>O2G</b>	All	No	N/A	N/A
<b>EDS/EPS/Pegasus</b>	All	No	N/A	N/A
<b>4059/IP 4059EE</b>	All	No	N/A	N/A
<b>OTEC (8770)</b>	All	No	N/A	N/A
<b>IPDongle (RPI)</b>	All	*	*	*
<b>OTSBC</b>	All	No	N/A	N/A
<b>OTCS</b>	All	No	N/A	N/A
<b>CCivr/CCS/CCA</b>	All	No	N/A	N/A
<b>ASM (Agent Selection Module)</b>	All	No	N/A	N/A
<b>TSAPI</b>	All	No	N/A	N/A
<b>Fax Server (OTFC)</b>	9.0 (3)	Yes	*	*
<b>ENS</b>	All	No	N/A	N/A
<b>IQ Messenger</b>	All	No	N/A	N/A
<b>OTNS</b>	All	Yes	*	Hotfix (4)
<b>Soft panel Manager</b>	All	No	N/A	N/A
<b>OmniPCX Record</b>	All	No	N/A	N/A
<b>IPDSP</b>	All	No	N/A	N/A
<b>ManageMyPhone</b>	All	No	N/A	N/A
<b>SelfCare</b>	All	No	N/A	N/A
<b>CMMI</b>	All	No	N/A	N/A
<b>MGS</b>	All	No	N/A	N/A
<b>SGA</b>	All	No	N/A	N/A
<b>AVBS</b>	All	No	N/A	N/A
<b>ClickToConnect</b>	All	No	N/A	N/A
<b>Calendar</b>	All	No	N/A	N/A
<b>Dispatch Console</b>	All	Yes	*	*



\* : analysis ongoing

3 <sup>rd</sup> P Product	Version	Affected	Impact	Remediation
<b>FlexLM</b>	All	No	N/A	N/A

## Status on Alcatel-Lucent Enterprise Network products

List of products and releases

Product	Version	Affected	Impact	Remediation
<b>PALM</b>	Cloud	No	N/A	N/A
<b>Subscription Manager</b>	Cloud	No	N/A	N/A
<b>Agnostic Data Lake</b>	Cloud	No	N/A	N/A
<b>Asset Tracking</b>	Cloud	Yes	*	*
<b>OV Cirrus</b>	10.1	Yes	Affected monitoring service has been stopped	*
<b>OV Cirrus</b>	4.6R1	No	N/A	N/A
<b>OV 2500</b>	4.6R1 or earlier	No	N/A	N/A
<b>Ucopia</b>	All	No	N/A	N/A
<b>Clearpass</b>	All	No	N/A	N/A
<b>OV3600</b>	All	No	N/A	N/A
<b>LBS</b>	Cloud	No	N/A	N/A
<b>RAP Appliance</b>	All	No	N/A	N/A
<b>NaaS</b>	Cloud	Yes	*	*
<b>Titan SD-WAN</b>	Cloud	No	N/A	N/A
<b>OmniSwitch</b>	All models except OS2220	No	N/A	N/A
<b>OmniSwitch</b>	OS2220	*	*	*
<b>OmniAccess Stellar AP</b>	All	No	N/A	N/A
<b>OmniAccess WLAN APs &amp; Controllers</b>	All	No	N/A	N/A

\* : analysis ongoing



## Status on Alcatel-Lucent Enterprise Cloud products

List of products and releases

Product	Version	Affected	Impact	Remediation
<b>Rainbow</b> <b>UCaaS/CPaaS/Edge/HDS/Hub</b>	All	No	N/A	N/A
<b>Rainbow Office</b>	<a href="https://www.ringcentral.com/trust-center/security-bulletin.html">https://www.ringcentral.com/trust-center/security-bulletin.html</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

- ALE will communicate on process to follow.
- For Customers, please contact your ALE Partner that can help you identifying the vulnerability impact and short-term remediation.

### (2) VNA

- Upgraded version to be delivered the 17<sup>th</sup> of Dec' 2021

### (3) OTFC

- OTFC version 7.6 is not vulnerable.
- Remediation for latest version is available. For partners, please refer to the corresponding bulletin available on MyPortal.

### (4) OTNS

- Hotfix available on Dec 17th '21

## History

Ed.01 (2021 December 13<sup>th</sup>): creation

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

Ed.03 (2021 December 14<sup>th</sup>): All solutions update, add of Rainbow Office

Ed.04 (2021 December 15<sup>h</sup>): CBD & NBD solutions updates

Ed.05 (2021 December 16<sup>h</sup>): CBD & NBD solutions updates, added reference to CVE-2021-45046.