Alcatel-Lucent Security Advisory No. SA-C0068 Ed. 08 - CVE-2021-44228 and following related to Log4j

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

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.

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*
OmniPCX Enterprise	All	No	N/A	N/A
OmniPCX Office/ OXO Connect/ OXO Connect Evolution	All	No	N/A	N/A
OMC /OHL/OLD PIMPhony/AST/Labetset	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)
GAS Server (WebRTCGW,OMS, OS)	All	No	N/A	N/A
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
4059/IP 4059EE	All	No	N/A	N/A
OTEC (8770)	All	No	N/A	N/A
IPDongle (RPi)	All	No	N/A	N/A
ALE Softphone	All	No	N/A	N/A
OTCPC Client	All	No	N/A	N/A
OTSBC	All	No	N/A	N/A
ALE Connect	All	No	N/A	N/A
OTCS	All	No	N/A	N/A
CCivr/CCS/CCA	All	No	N/A	N/A
ASM (Agent Selection Module)	All	No	N/A	N/A
TSAPI	All	No	N/A	N/A
Fax Server (OTFC)	9.0 (3)	Yes	*	*
ENS	All	No	N/A	N/A
IQ Messenger	*	Yes	*	(4)
Soft panel Manager	All	No	N/A	N/A
OmniPCX Record	All	No	N/A	N/A
IPDSP	All	No	No	(5)
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	*	*
TAPI	All	No	N/A	N/A

** : analysis ongoing*

3rd P Product	Version	Affected	Impact	Remediation
FlexLM	All	No	N/A	N/A

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	Yes	*	*
OV Cirrus	10.1	Yes	Affected monitoring service has been stopped	*
OV Cirrus	4.6R1	No	N/A	N/A
OV 2500	4.6R1 or earlier	No	N/A	N/A
Ucopia	All	No	N/A	N/A
Clearpass	All	No	N/A	N/A
OV3600	All	No	N/A	N/A
LBS	Cloud	No	N/A	N/A
RAP Appliance	All	No	N/A	N/A
NaaS	Cloud	Yes	*	*
Titan SD-WAN	Cloud	No	N/A	N/A
OmniSwitch	All models except OS2220	No	N/A	N/A
OmniSwitch	OS2220	*	*	*
OmniAccess Stellar AP	All	No	N/A	N/A
OmniAccess WLAN APs & Controllers	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
Rainbow UCaaS/CPaaS/Edge/HDS/Hub	All	No	N/A	N/A
Rainbow Office	https://www.ringcentral.com/trust-center/security-bulletin.html			

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 has communicated on process to follow for Business Partners. Please refer to Technical Communication TC2930.
- For Customers, please contact your ALE Partner that will help you identifying the vulnerability impact and short-term remediation.

(2) VNA

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

(3) OTFC

- OTFC version 7.6 is not vulnerable.
- Remediation for latest version is available (R9.0.0.663). For partners, please refer to the corresponding TKC bulletin available on MyPortal.

(4) IQ Messenger

- Fix version will be 11.3.1, available the 20th Dec’ 21 (embed log4j R2.16)
- ALE has communicated on process to follow.
- For Customers, please contact your ALE Partner that will help you to apply remediation.

(5) IPDSP

- Following further R&D analysis, IPDSP using log4J , all IPDSP versions are not affected by CVE-2021-45046 & CVE-2021-44228

History

Ed.01 (2021 December 13th): creation

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

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

Ed.04 (2021 December 15h): CBD & NBD solutions updates

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

Ed.06 (2021 December 17h):.CBD solutions updates

Ed07 (2021 December 21st) : CBD solutions updates

Ed08 (2021 December 22st) : CBD solutions updates