



Alcatel-Lucent Security Advisory No. SA-C0066 Ed. 01

OTMS remote code execution - CVE-2020-11794

Summary

A vulnerability has been discovered in OpenTouch Multimedia Services, making it possible for an attacker with administration rights to execute code on the server via web requests with high privileges.

References

Reference: CVE-2020-11794

Date: April 15th, 2020

Risk: High

Impact: Get access

Attack expertise: Skilled, Administrative user

Attack requirements: Remote

CVSS score: 8.0 (HIGH)

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11794>

Description of the vulnerability

Cgi script vmconstruct.cgi is vulnerable to shell command injection attacks through HTTP POST request.

An attacker with an OT administrator cookie can inject arbitrary OS command using semicolon (;) character in the web request.

Impacts

OS command injection vulnerabilities can lead to elevate shell access on OT server for the attacker.

Status on Alcatel-Lucent Enterprise products

List of products and releases concerned (or affected)

Product Name	Release
OT	Before R2.5 MD3

List of products and releases NOT concerned (or affected)

Product Name	Release
OT	R2.5 MD3

Resolution for Alcatel-Lucent Enterprise affected products

A Hotfix is available for current OT R2.5MD1 : [ALF0001585662280281](#)

Product	Fixed in	Date
OT	R2.5 MD3	May 07 th , 2020

Acknowledgement

Alcatel-Lucent Enterprise would like to thank Mr. Michal Błaszczak for its precious help reporting this vulnerability and making it possible for us to continuously improve the security of our products.

History

Ed.01 (2020 April 20st): creation