Alcatel-Lucent Security Advisory No. SA-C0066 Ed. 03
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
OT	R2.6

List of products and releases NOT concerned (or affected)

Product Name	Release
OT	R2.5 MD3
OT	R2.6 MD1

Resolution for Alcatel-Lucent Enterprise affected products

Hotfix is available for current OT R2.5MD1: ALF0001585662280281
Hotfix is available for OT2.5 MD2 (OTBE): ALF0001590672086131
Hotfix is available for OT2.6: ALF0001590580347534

Product	Fixed in	Date
OT	R2.5 MD3	May 07th, 2020
OT	R2.6 MD1	Availability date to precise
OT	R<2.5	No specific patch will be delivered for OT release prior 2.5. It is recommended to migrate to OT R2.5MD3 in such case

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 20th): creation

Ed.02 (2020 May 26th): clarification for R2.6 & release prior 2.5

Ed.03 (2020 June 8th): patch references for R2.6 & R2.5MD2