iControl REST and TMSH vulnerability

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-40698
State	PUBLISHED
Assigner	f5
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-13 16:16:43 UTC
Updated	2026-05-13 16:27:11 UTC
Description	A vulnerability exists in BIG-IP and BIG-IQ systems where a highly privileged, authenticated attacker with at least the Resou

Risk And Classification

Primary CVSS: v4.0 8.5 HIGH from f5sirt@f5.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-77 | CWE-77 CWE-77 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Version	Source	Type	Score	Severity	Vector
4.0	f5sirt@f5.com	Secondary	8.5	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:X/C...
4.0	CNA	CVSS	8.5	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N
3.1	f5sirt@f5.com	Primary	8.7	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:N
3.1	CNA	CVSS	8.7	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:N
3.1	CNA	CVSS	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

None

Confidentiality

High

Integrity

High

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

None

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:N

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	F5	BIG-IP	unaffected 21.1.0 * custom	Not specified
CNA	F5	BIG-IP	affected 21.0.0 21.0.0.2 custom	Not specified
CNA	F5	BIG-IP	affected 17.5.0 17.5.1.6 custom	Not specified
CNA	F5	BIG-IP	affected 17.1.0 17.1.3.2 custom	Not specified

CNA	F5	BIG-IP	affected 16.1.0 * custom	Not specified
CNA	F5	BIG-IQ	affected 8.4.0 * custom	Not specified

References

Reference	Source	Link	Tags
my.f5.com/manage/s/article/K000160981	f5sirt@f5.com	my.f5.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: F5 (en)

There are currently no legacy QID mappings associated with this CVE.