



# iControl REST and TMSH vulnerability

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

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

## 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/MSX/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/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
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/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/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/MSX/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	<a href="https://my.f5.com">my.f5.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

## Vendor Comments And Credit

Discovery Credit

**CNA: F5** (en)

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

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.cve.org). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses/mitre).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)