



iControl SOAP vulnerability

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

Summary

CVE	CVE-2026-35062
State	PUBLISHED
Assigner	f5
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-13 16:16:40 UTC
Updated	2026-05-13 16:27:11 UTC
Description	An authenticated iControl SOAP user may be able to obtain information of other accounts. Note: Software versions which f

Risk And Classification

Primary CVSS: v4.0 7.1 HIGH from f5sirt@f5.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/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

EPSS: 0.000500000 probability, percentile 0.157810000 (date 2026-05-17)

Problem Types: CWE-266 | CWE-266 CWE-266 Incorrect Privilege Assignment.

Version	Source	Type	Score	Severity	Vector
4.0	f5sirt@f5.com	Secondary	7.1	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/C...
4.0	CNA	CVSS	7.1	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N
3.1	f5sirt@f5.com	Primary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
3.1	CNA	CVSS	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

High

Integrity

None

Availability

None

Sub Conf.

None

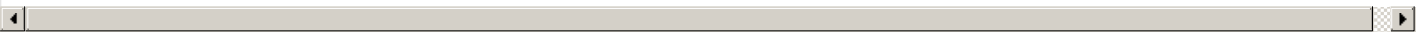
Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/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/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

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/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 21.0.0.1 custom	Not specified
CNA	F5	BIG-IP	affected 17.5.1 17.5.1.4 custom	Not specified
CNA	F5	BIG-IP	affected 17.1.0 17.1.3.1 custom	Not specified
CNA	F5	BIG-IP	affected 16.1.0 * custom	Not specified

CNA	F5	DIG-IP	affected 10.1.1.0	custom	not specified
References					
Reference	Source	Link	Tags		
my.f5.com/manage/s/article/K000159021	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.					

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

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

CVE.report and Source URL Uptime Status [status.cve.report](#)