



CVE-2016-5024

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2016-5024
State	PUBLISHED
Assigner	f5
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-01-03 21:59:00 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Virtual servers in F5 BIG-IP systems 11.6.1 before 11.6.1 HF1 and 12.1.x before 12.1.2, when configured to parse RADIUS

Risk And Classification

Primary CVSS: v3.0 5.9 MEDIUM from nvd@nist.gov

CVSS: 3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

EPSS: 0.017070000 probability, percentile 0.824510000 (date 2026-05-11)

Problem Types: CWE-20 | iRules RADIUS message parsing vulnerability

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	5.9	MEDIUM	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
2.0	nvd@nist.gov	Primary	4.3		AV:N/AC:M/Au:N/C:N/I:N/A:P

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

None

Availability

High

CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/AC:M/Au:N/C:N/I:N/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	F5	Big-ip Access Policy Manager	11.6.1	All	All	All
Application	F5	Big-ip Access Policy Manager	12.1.0	All	All	All
Application	F5	Big-ip Access Policy Manager	12.1.1	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	11.6.1	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	12.1.0	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	12.1.1	All	All	All
Application	F5	Big-ip Analytics	11.6.1	All	All	All
Application	F5	Big-ip Analytics	12.1.0	All	All	All
Application	F5	Big-ip Analytics	12.1.1	All	All	All
Application	F5	Big-ip Application Acceleration Manager	11.6.1	All	All	All
Application	F5	Big-ip Application Acceleration Manager	12.1.0	All	All	All
Application	F5	Big-ip Application Acceleration Manager	12.1.1	All	All	All
Application	F5	Big-ip Application Security Manager	11.6.1	All	All	All
Application	F5	Big-ip Application Security Manager	12.1.0	All	All	All
Application	F5	Big-ip Application Security Manager	12.1.1	All	All	All
Application	F5	Big-ip Domain Name System	12.1.0	All	All	All

Application	F5	Big-ip Domain Name System	12.1.1	All	All	All
Application	F5	Big-ip Global Traffic Manager	11.6.1	All	All	All
Application	F5	Big-ip Link Controller	11.6.1	All	All	All
Application	F5	Big-ip Link Controller	12.1.0	All	All	All
Application	F5	Big-ip Link Controller	12.1.1	All	All	All
Application	F5	Big-ip Local Traffic Manager	11.6.1	All	All	All
Application	F5	Big-ip Local Traffic Manager	12.1.0	All	All	All
Application	F5	Big-ip Local Traffic Manager	12.1.1	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	11.6.1	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	12.1.0	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	12.1.1	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	F5 Networks	F5 BIG-IP LTM AAM AFM Analytics APM ASM DNS GTM Link Controller PEM	affected 11.6.1 before 11.6.1 HF1

References

Reference	Source
F5 BIG-IP iRule Processing Bug Lets Remote Users Cause the Target Service to Restart - SecurityTracker	af854a3a-2127-422b-91ae-364c
support.f5.com/csp	af854a3a-2127-422b-91ae-364c
Multiple F5 BIG-IP Products CVE-2016-5024 Denial of Service Vulnerability	af854a3a-2127-422b-91ae-364c
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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](#)