



CVE-2022-28716

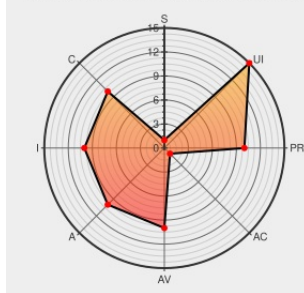
Published on: Not Yet Published

Last Modified on: 01/24/2023 03:37:00 PM UTC

CVE-2022-28716

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H



Certain versions of [Big-ip Advanced Firewall Manager](#) from [F5](#) contain the following vulnerability:

On 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, and all versions of 12.1.x 11.6.x, a DOM-based cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP AFM, CGNAT, and PEM Configuration utility that allows an attacker to execute

JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated

CVE-2022-28716 has been assigned by [f5sirt@f5.com](#) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
No Description Provided	CVE-2022-28716	MICO support f5.com/en/articles/005451852

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

[377807](#) F5 BIG-IP AFM,CGNAT,PEM TMUI Cross-Site Scripting (XSS) Vulnerability (K25451853)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	F5	Big-ip Advanced Firewall Manager	All	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	All	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	All	All	All	All
Application	F5	Big-ip Carrier-grade Nat	All	All	All	All
Application	F5	Big-ip Carrier-grade Nat	All	All	All	All
Application	F5	Big-ip Carrier-grade Nat	All	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	All	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	All	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	All	All	All	All
cpe:2.3:a:f5:big-ip_advanced_firewall_manager:*****:.*:						
cpe:2.3:a:f5:big-ip_advanced_firewall_manager:*****:.*:						
cpe:2.3:a:f5:big-ip_advanced_firewall_manager:*****:.*:						
cpe:2.3:a:f5:big-ip_carrier-grade_nat:*****:.*:						
cpe:2.3:a:f5:big-ip_carrier-grade_nat:*****:.*:						
cpe:2.3:a:f5:big-ip_carrier-grade_nat:*****:.*:						
cpe:2.3:a:f5:big-ip_policy_enforcement_manager:*****:.*:						
cpe:2.3:a:f5:big-ip_policy_enforcement_manager:*****:.*:						
cpe:2.3:a:f5:big-ip_policy_enforcement_manager:*****:.*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
	F5 BIG-IP (AFM, CGNAT, PEM) cross-site scripting CVE-2022-28716 - redpacketsecurity.com/f5-	2022-05-05

@RedPacketSec	big-ip-afm-...	10:02:02
 @CVEreport	CVE-2022-28716 : On 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to... twitter.com/i/web/status/1...	2022-05-05 17:19:46
 @RedPacketSec	F5 BIG-IP (AFM, CGNAT, PEM) cross-site scripting CVE-2022-28716 - redpacketsecurity.com/f5-big-ip-afm-...	2022-05-06 10:01:40
 /r/netcve	CVE-2022-28716	2022-05-05 17:38:52
 /r/k12cybersecurity	MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in F5Networks Products Could Allow for Arbitrary Code Execution - PATCH: NOW	2022-05-06 14:11:01
 /r/k12cybersecurity	UPDATED MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in F5Networks Products Could Allow for Arbitrary Code Execution - PATCH: NOW	2022-05-09 13:34:10
 /r/k12cybersecurity	UPDATED MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in F5Networks Products Could Allow for Arbitrary Code Execution - PATCH: NOW	2022-05-11 16:42:45
← Previous ID		Next ID→

© CVE.report 2023   |

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.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report