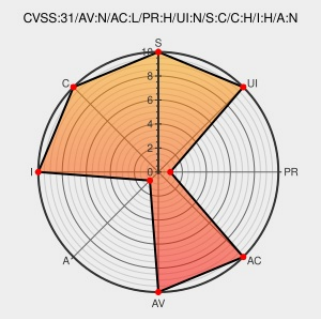
CVE-2022-27806

Published on: Not Yet Published

Last Modified on: 05/13/2022 04:48:00 PM UTC

CVE-2022-27806

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Big-ip Access Policy Manager from F5 contain the following vulnerability:

On all versions of 16.1.x, 15.1.x, 14.1.x, 13.1.x, 12.1.x, and 11.6.x of F5 BIG-IP Advanced WAF, ASM, and ASM, and F5 BIG-IP Guided Configuration (GC) all versions prior to 9.0, when running in Appliance mode, an authenticated attacker assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing command injection vulnerabilities in undisclosed URIs in F5 BIG-IP Guided Configuration. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated

CVE-2022-27806 has been assigned by f5sirt@f5.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.2 - HIGH

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

CVSS2 Score: 6 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
No Description Provided.	support.f5.com	MISC support.f5.com/csp/article/K68647001

No Description Provided | support.f5.com text/html | MISC support.f5.com/csp/article/K68647001

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

376593 F5 BIG-IP Application Security Manager (ASM), Access Policy Manager (APM) Restriction Bypass Vulnerability (K68647001)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	F5	Big-ip Access Policy Manager	13.1.0	All	All	All
Application	F5	Big-ip Access Policy Manager	13.1.1	All	All	All
Application	F5	Big-ip Access Policy Manager	13.1.3	All	All	All
Application	F5	Big-ip Access Policy Manager	13.1.4	All	All	All
Application	F5	Big-ip Access Policy Manager	13.1.5	All	All	All
Application	F5	Big-ip Access Policy Manager	14.1.0	All	All	All
Application	F5	Big-ip Access Policy Manager	14.1.2	All	All	All
Application	F5	Big-ip Access Policy Manager	14.1.3	All	All	All
Application	F5	Big-ip Access Policy Manager	14.1.4	All	All	All
Application	F5	Big-ip Access Policy Manager	15.1.0	All	All	All
Application	F5	Big-ip Access Policy Manager	15.1.1	All	All	All
Application	F5	Big-ip Access Policy Manager	15.1.2	All	All	All
Application	F5	Big-ip Access Policy Manager	15.1.3	All	All	All
Application	F5	Big-ip Access Policy Manager	15.1.4	All	All	All
Application	F5	Big-ip Access Policy Manager	15.1.5	All	All	All
Application	F5	Big-ip Access Policy Manager	16.1.0	All	All	All
Application	F5	Big-ip Access Policy Manager	16.1.1	All	All	All
Application	F5	Big-ip Access Policy Manager	16.1.2	All	All	All
Application	F5	Big-ip Advanced Web Application Firewall	13.1.0	All	All	All
Application	F5	Big-ip Advanced Web Application Firewall	13.1.1	All	All	All
Application	F5	Big-ip Advanced Web Application Firewall	13.1.3	All	All	All
Application	F5	Big-ip Advanced Web Application Firewall	13.1.4	All	All	All
Application	F5	Big-ip Advanced Web Application Firewall	13.1.5	All	All	All
Application	F5	Big-ip Advanced Web Application Firewall	14.1.0	All	All	All
Application	F5	Big-ip Advanced Web Application Firewall	14.1.2	All	All	All
Application	F5	Big-ip Advanced Web Application Firewall	14.1.3	All	All	All

Application	F5	Big-ip Advanced Web Application Firewall	14.1.4	All	All	All
Application	F5	Big-ip Advanced Web Application Firewall	15.1.0	All	All	All
Application	F5	Big-ip Advanced Web Application Firewall	15.1.1	All	All	All
Application	F5	Big-ip Advanced Web Application Firewall	15.1.2	All	All	All
Application	F5	Big-ip Advanced Web Application Firewall	15.1.3	All	All	All
Application	F5	Big-ip Advanced Web Application Firewall	15.1.4	All	All	All
Application	F5	Big-ip Advanced Web Application Firewall	15.1.5	All	All	All
Application	F5	Big-ip Advanced Web Application Firewall	16.1.0	All	All	All
Application	F5	Big-ip Advanced Web Application Firewall	16.1.1	All	All	All
Application	F5	Big-ip Advanced Web Application Firewall	16.1.2	All	All	All
Application	F5	Big-ip Application Security Manager	13.1.0	All	All	All
Application	F5	Big-ip Application Security Manager	13.1.1	All	All	All
Application	F5	Big-ip Application Security Manager	13.1.3	All	All	All
Application	F5	Big-ip Application Security Manager	13.1.4	All	All	All
Application	F5	Big-ip Application Security Manager	13.1.5	All	All	All
Application	F5	Big-ip Application Security Manager	14.1.0	All	All	All
Application	F5	Big-ip Application Security Manager	14.1.2	All	All	All
Application	F5	Big-ip Application Security Manager	14.1.3	All	All	All
Application	F5	Big-ip Application Security Manager	14.1.4	All	All	All
Application	F5	Big-ip Application Security Manager	15.1.0	All	All	All
Application	F5	Big-ip Application Security Manager	15.1.1	All	All	All
Application	F5	Big-ip Application Security Manager	15.1.2	All	All	All
Application	F5	Big-ip Application Security Manager	15.1.3	All	All	All
Application	F5	Big-ip Application Security Manager	15.1.4	All	All	All
Application	F5	Big-ip Application Security Manager	15.1.5	All	All	All
Application	F5	Big-ip Application Security Manager	16.1.0	All	All	All
Application	F5	Big-ip Application Security Manager	16.1.1	All	All	All
Application	F5	Big-ip Application Security Manager	16.1.2	All	All	All
Application	F5	Big-ip Guided Configuration	All	All	All	All

cpe:2.3:a:f5:big-ip_access_policy_manager:13.1.0:*:*:*:*:*:*:*

cpe:2.3:a:f5:big-ip_access_policy_manager:13.1.1:*:*:*:*:*:*:*

cpe:2.3:a:f5:big-ip_access_policy_manager:13.1.3:*:*:*:*:*:*:*

cpe:2.3:a:f5:big-ip_access_policy_manager:13.1.4:*:*:*:*:*:*:*

cpe:2.3:a:f5:big-ip_access_policy_manager:13.1.5:*:*:*:*:*:*:*

cpe:2.3:a:f5:big-ip_access_policy_manager:14.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_access_policy_manager:14.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_access_policy_manager:14.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_access_policy_manager:14.1.4:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_access_policy_manager:15.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_access_policy_manager:15.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_access_policy_manager:15.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_access_policy_manager:15.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_access_policy_manager:15.1.4:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_access_policy_manager:15.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_access_policy_manager:16.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_access_policy_manager:16.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_access_policy_manager:16.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_advanced_web_application_firewall:13.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_advanced_web_application_firewall:13.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_advanced_web_application_firewall:13.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_advanced_web_application_firewall:13.1.4:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_advanced_web_application_firewall:13.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_advanced_web_application_firewall:14.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_advanced_web_application_firewall:14.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_advanced_web_application_firewall:14.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_advanced_web_application_firewall:14.1.4:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_advanced_web_application_firewall:15.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_advanced_web_application_firewall:15.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_advanced_web_application_firewall:15.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_advanced_web_application_firewall:15.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_advanced_web_application_firewall:15.1.4:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_advanced_web_application_firewall:15.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_advanced_web_application_firewall:16.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_advanced_web_application_firewall:16.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_advanced_web_application_firewall:16.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_security_manager:13.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_security_manager:13.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_security_manager:13.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_security_manager:13.1.4:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_security_manager:13.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_security_manager:14.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_security_manager:14.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_security_manager:14.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_security_manager:14.1.4:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_security_manager:15.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_security_manager:15.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_security_manager:15.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_security_manager:15.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_security_manager:15.1.4:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_security_manager:15.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_security_manager:16.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_security_manager:16.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_application_security_manager:16.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_guided_configuration:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@RedPacketSec	F5 BIG-IP security bypass | CVE-2022-27806 - redpacketsecurity.com/f5-big-ip-secu…	2022-05-05 10:02:02
@CVEreport	CVE-2022-27806 : On all versions of 16.1.x, 15.1.x, 14.1.x, 13.1.x, 12.1.x, and 11.6.x of F5 BIG-IP Advanced WAF, A… twitter.com/i/web/status/1…	2022-05-05 17:13:25
	MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in F5Networks Products Could	2022-05-06

/r/k12cybersecurity	Allow for Arbitrary Code Execution - PATCH: NOW	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→