

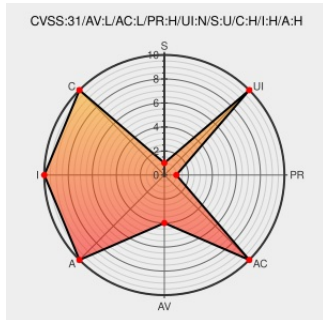


CVE-2022-33962

Published on: Not Yet Published

Last Modified on: 08/10/2022 11:42:00 PM UTC

CVE-2022-33962

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

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

In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

CVE-2022-33962 has been assigned by [f5sirt@f5.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [F5](#) - **BIG-IP** version **>= 13.1.0**

Affected Vendor/Software: [F5](#) - **BIG-IP** version **< 14.1.5.1**

Affected Vendor/Software: [F5](#) - **BIG-IP** version **< 15.1.6.1**

Affected Vendor/Software: [F5](#) - **BIG-IP** version **< 16.1.3.1**

Affected Vendor/Software: [F5](#) - **BIG-IP** version **< 17.0.0.1**

CVSS3 Score: **6.7 - MEDIUM**

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

CVE References

Description	Tags	Link
No Description Provided	support.f5.com text/html	MISC support.f5.com/csp/article/K80970653

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

[376793](#) F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) Big-ip Irules Vulnerability [cve-2022-33962](#) (K80970653)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	F5	Big-ip Access Policy Manager	All	All	All	All
Application	F5	Big-ip Access Policy Manager	17.0.0	All	All	All
Application	F5	Big-ip Access Policy Manager	All	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	All	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	17.0.0	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	All	All	All	All
Application	F5	Big-ip Analytics	All	All	All	All
Application	F5	Big-ip Analytics	17.0.0	All	All	All
Application	F5	Big-ip Analytics	All	All	All	All
Application	F5	Big-ip Application Acceleration Manager	All	All	All	All
Application	F5	Big-ip Application Acceleration Manager	17.0.0	All	All	All
Application	F5	Big-ip Application Acceleration Manager	All	All	All	All
Application	F5	Big-ip Application Security Manager	All	All	All	All
Application	F5	Big-ip Application Security Manager	17.0.0	All	All	All
Application	F5	Big-ip Application Security Manager	All	All	All	All
Application	F5	Big-ip Domain Name System	All	All	All	All
Application	F5	Big-ip Domain Name System	17.0.0	All	All	All
Application	F5	Big-ip Domain Name System	All	All	All	All
Application	F5	Big-ip Fraud Protection Service	All	All	All	All
Application	F5	Big-ip Fraud Protection Service	17.0.0	All	All	All
Application	F5	Big-ip Fraud Protection Service	All	All	All	All
Application	F5	Big-ip Global Traffic Manager	All	All	All	All
Application	F5	Big-ip Global Traffic Manager	17.0.0	All	All	All
Application	F5	Big-ip Global Traffic Manager	All	All	All	All
Application	F5	Big-ip Link Controller	All	All	All	All
Application	F5	Big-ip Link Controller	17.0.0	All	All	All

Application	F5	Big-ip Link Controller	All	All	All	All
Application	F5	Big-ip Local Traffic Manager	All	All	All	All
Application	F5	Big-ip Local Traffic Manager	17.0.0	All	All	All
Application	F5	Big-ip Local Traffic Manager	All	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	All	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	17.0.0	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	All	All	All	All
cpe:2.3:a:f5:big-ip_access_policy_manager:*****:						
cpe:2.3:a:f5:big-ip_access_policy_manager:17.0.0:*****:						
cpe:2.3:a:f5:big-ip_access_policy_manager:*****:						
cpe:2.3:a:f5:big-ip_advanced_firewall_manager:*****:						
cpe:2.3:a:f5:big-ip_advanced_firewall_manager:17.0.0:*****:						
cpe:2.3:a:f5:big-ip_advanced_firewall_manager:*****:						
cpe:2.3:a:f5:big-ip_analytics:*****:						
cpe:2.3:a:f5:big-ip_analytics:17.0.0:*****:						
cpe:2.3:a:f5:big-ip_analytics:*****:						
cpe:2.3:a:f5:big-ip_application_acceleration_manager:*****:						
cpe:2.3:a:f5:big-ip_application_acceleration_manager:17.0.0:*****:						
cpe:2.3:a:f5:big-ip_application_acceleration_manager:*****:						
cpe:2.3:a:f5:big-ip_application_security_manager:*****:						
cpe:2.3:a:f5:big-ip_application_security_manager:17.0.0:*****:						
cpe:2.3:a:f5:big-ip_application_security_manager:*****:						
cpe:2.3:a:f5:big-ip_domain_name_system:*****:						
cpe:2.3:a:f5:big-ip_domain_name_system:17.0.0:*****:						
cpe:2.3:a:f5:big-ip_domain_name_system:*****:						
cpe:2.3:a:f5:big-ip_fraud_protection_service:*****:						
cpe:2.3:a:f5:big-ip_fraud_protection_service:17.0.0:*****:						
cpe:2.3:a:f5:big-ip_fraud_protection_service:*****:						
cpe:2.3:a:f5:big-ip_global_traffic_manager:*****:						
cpe:2.3:a:f5:big-ip_global_traffic_manager:17.0.0:*****:						

cpe:2.3:a:f5:big-ip_global_traffic_manager:17.0.0:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_global_traffic_manager:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_link_controller:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_link_controller:17.0.0:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_link_controller:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_local_traffic_manager:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_local_traffic_manager:17.0.0:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_local_traffic_manager:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_policy_enforcement_manager:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_policy_enforcement_manager:17.0.0:*:*:*:*:*:
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)
 @CVEreport	CVE-2022-33962 : In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x... twitter.com/i/web/status/1...	2022-08-04 17:54:30
 @sidfm_jp	F5 Networks BIG-IP の iRules に任意のコマンドを実行される問題 (CVE-2022-33962) [42979] sid.softek.jp/content/show/4... #SIDfm #脆弱性情報	2022-08-08 07:30:02

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

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