



CVE-2023-22323

Published on: Not Yet Published

Last Modified on: 02/09/2023 06:13:00 PM UTC

CVE-2023-22323

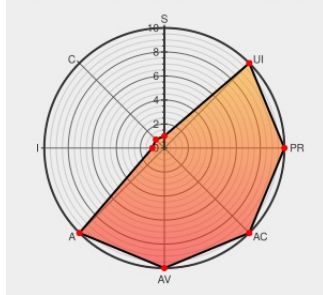
[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)

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



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

In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, and all versions of 13.1.x, when OSCP authentication profile is configured on a virtual server, undisclosed requests can cause an increase in CPU resource utilization. Note: Software versions which have reached End of

Technical Support (EoTS) are not evaluated.

CVE-2023-22323 has been assigned by f5sirt@f5.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **F5 - BIG-IP** version = **17.0.0**

Affected Vendor/Software: **F5 - BIG-IP** version = **16.1.0**

Affected Vendor/Software: **F5 - BIG-IP** version = **15.1.0**

Affected Vendor/Software: **F5 - BIG-IP** version = **14.1.0**

Affected Vendor/Software: **F5 - BIG-IP** version = **13.1.0**

CVSS3 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
myF5	my.f5.com text/html	MISC my.f5.com/manage/s/article/K56412001

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

377969 F5 BIG-IP OSCP Authentication Profile Vulnerability CVE-2023-22323 (K56412001)

Exploit/POC from Github

In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x before 14.1.5.3, an...

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	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 Analytics	All	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	All	All	All	All
Application	F5	Big-ip Application Security Manager	All	All	All	All
Application	F5	Big-ip Application Security Manager	All	All	All	All
Application	F5	Big-ip Ddos Hybrid Defender	All	All	All	All
Application	F5	Big-ip Ddos Hybrid Defender	All	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	All	All	All	All
Application	F5	Big-ip Link Controller	All	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	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 Ssl Orchestrator	All	All	All	All

Application	F5	Big-ip Ssl Orchestrator	All	All	All	All
cpe:2.3:a:f5:big-ip_access_policy_manager:*****:						
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:*****:						
cpe:2.3:a:f5:big-ip_analytics:*****:						
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:*****:						
cpe:2.3:a:f5:big-ip_application_security_manager:*****:						
cpe:2.3:a:f5:big-ip_application_security_manager:*****:						
cpe:2.3:a:f5:big-ip_ddos_hybrid_defender:*****:						
cpe:2.3:a:f5:big-ip_ddos_hybrid_defender:*****:						
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:*****:						
cpe:2.3:a:f5:big-ip_link_controller:*****:						
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:*****:						
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_ssl_orchestrator:*****:						
cpe:2.3:a:f5:big-ip_ssl_orchestrator:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVereport	CVE-2023-22323 : In BIP-IP versions 17.0.x before 17.0.0.2, 16.1.x before 16.1.3.3, 15.1.x before 15.1.8.1, 14.1.x... twitter.com/i/web/status/1...	2023-02-01 18:07:54

[← 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](#)