



CVE-2017-6131

Published on: 05/23/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:50 PM UTC

CVE-2017-6131

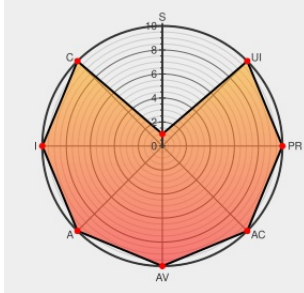
Source: Mitre

Source: NIST

CVE.ORG

Print: PDF

CVSS:30/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



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

In some circumstances, an F5 BIG-IP version 12.0.0 to 12.1.2 and 13.0.0 Azure cloud instance may contain a default administrative password which could be used to remotely log into the BIG-IP system. The impacted administrative account is the Azure instance administrative user that was created at deployment. The root and

admin accounts are not vulnerable. An attacker may be able to remotely access the BIG-IP host via SSH.

CVE-2017-6131 has been assigned by f5sirt@f5.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: **F5 Networks, Inc. - BIG-IP Azure cloud instance** version **12.0.0 to 12.1.2**

Affected Vendor/Software: **F5 Networks, Inc. - BIG-IP Azure cloud instance** version **13.0.0**

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
F5 BIG-IP Virtual Edition Azure Default Password Lets Remote Users Access the Target System - SecurityTracker	www.securitytracker.com text/html	 SECTRACK 1038569
No Description Provided	Permissions Required Vendor Advisory support.f5.com text/html	 CONFIRM support.f5.com/csp/article/K61757346

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	F5	Big-ip Access Policy Manager	12.0.0	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 Access Policy Manager	12.1.2	All	All	All
Application	F5	Big-ip Access Policy Manager	13.0.0	All	All	All
Application	F5	Big-ip Access Policy Manager	12.0.0	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 Access Policy Manager	12.1.2	All	All	All
Application	F5	Big-ip Access Policy Manager	13.0.0	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	12.0.0	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 Advanced Firewall Manager	12.1.2	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	13.0.0	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	12.0.0	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 Advanced Firewall Manager	12.1.2	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	13.0.0	All	All	All
Application	F5	Big-ip Application Acceleration Manager	12.0.0	All	All	All

[illegible]

Application	F5	Big-ip Link Controller	12.1.1	All	All	All
Application	F5	Big-ip Link Controller	12.1.2	All	All	All
Application	F5	Big-ip Link Controller	13.0.0	All	All	All
Application	F5	Big-ip Local Traffic Manager	12.0.0	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 Local Traffic Manager	12.1.2	All	All	All
Application	F5	Big-ip Local Traffic Manager	13.0.0	All	All	All
Application	F5	Big-ip Local Traffic Manager	12.0.0	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 Local Traffic Manager	12.1.2	All	All	All
Application	F5	Big-ip Local Traffic Manager	13.0.0	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	12.0.0	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
Application	F5	Big-ip Policy Enforcement Manager	12.1.2	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	13.0.0	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	12.0.0	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
Application	F5	Big-ip Policy Enforcement Manager	12.1.2	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	13.0.0	All	All	All
Application	F5	Big-ip Websafe	12.0.0	All	All	All
Application	F5	Big-ip Websafe	12.1.0	All	All	All
Application	F5	Big-ip Websafe	12.1.1	All	All	All
Application	F5	Big-ip Websafe	12.1.2	All	All	All
Application	F5	Big-ip Websafe	13.0.0	All	All	All
Application	F5	Big-ip Websafe	12.0.0	All	All	All
Application	F5	Big-ip Websafe	12.1.0	All	All	All
Application	F5	Big-ip Websafe	12.1.1	All	All	All
Application	F5	Big-ip Websafe	12.1.2	All	All	All
Application	F5	Big-ip Websafe	13.0.0	All	All	All

cpe:2.3:a:f5:big-ip_access_policy_manager:12.0.0:*****:

cpe:2.3:a:f5:biq-ip access policy manager:12.1.0:*****:

cpe:2.3:a:f5:big-ip_access_policy_manager:12.1.1:****:****:
cpe:2.3:a:f5:big-ip_access_policy_manager:12.1.2:****:****:
cpe:2.3:a:f5:big-ip_access_policy_manager:13.0.0:****:****:
cpe:2.3:a:f5:big-ip_access_policy_manager:12.0.0:****:****:
cpe:2.3:a:f5:big-ip_access_policy_manager:12.1.0:****:****:
cpe:2.3:a:f5:big-ip_access_policy_manager:12.1.1:****:****:
cpe:2.3:a:f5:big-ip_access_policy_manager:12.1.2:****:****:
cpe:2.3:a:f5:big-ip_access_policy_manager:13.0.0:****:****:
cpe:2.3:a:f5:big-ip_advanced_firewall_manager:12.0.0:****:****:
cpe:2.3:a:f5:big-ip_advanced_firewall_manager:12.1.0:****:****:
cpe:2.3:a:f5:big-ip_advanced_firewall_manager:12.1.1:****:****:
cpe:2.3:a:f5:big-ip_advanced_firewall_manager:12.1.2:****:****:
cpe:2.3:a:f5:big-ip_advanced_firewall_manager:13.0.0:****:****:
cpe:2.3:a:f5:big-ip_advanced_firewall_manager:12.0.0:****:****:
cpe:2.3:a:f5:big-ip_advanced_firewall_manager:12.1.0:****:****:
cpe:2.3:a:f5:big-ip_advanced_firewall_manager:12.1.1:****:****:
cpe:2.3:a:f5:big-ip_advanced_firewall_manager:12.1.2:****:****:
cpe:2.3:a:f5:big-ip_advanced_firewall_manager:13.0.0:****:****:
cpe:2.3:a:f5:big-ip_application_acceleration_manager:12.0.0:****:****:
cpe:2.3:a:f5:big-ip_application_acceleration_manager:12.1.0:****:****:
cpe:2.3:a:f5:big-ip_application_acceleration_manager:12.1.1:****:****:
cpe:2.3:a:f5:big-ip_application_acceleration_manager:12.1.2:****:****:
cpe:2.3:a:f5:big-ip_application_acceleration_manager:13.0.0:****:****:
cpe:2.3:a:f5:big-ip_application_acceleration_manager:12.0.0:****:****:
cpe:2.3:a:f5:big-ip_application_acceleration_manager:12.1.0:****:****:
cpe:2.3:a:f5:big-ip_application_acceleration_manager:12.1.1:****:****:
cpe:2.3:a:f5:big-ip_application_acceleration_manager:12.1.2:****:****:
cpe:2.3:a:f5:big-ip_application_acceleration_manager:13.0.0:****:****:

cpe:2.3:a:f5:big-ip_application_security_manager:12.0.0:****:
cpe:2.3:a:f5:big-ip_application_security_manager:12.1.0:****:
cpe:2.3:a:f5:big-ip_application_security_manager:12.1.1:****:
cpe:2.3:a:f5:big-ip_application_security_manager:12.1.2:****:
cpe:2.3:a:f5:big-ip_application_security_manager:13.0.0:****:
cpe:2.3:a:f5:big-ip_application_security_manager:12.0.0:****:
cpe:2.3:a:f5:big-ip_application_security_manager:12.1.0:****:
cpe:2.3:a:f5:big-ip_application_security_manager:12.1.1:****:
cpe:2.3:a:f5:big-ip_application_security_manager:12.1.2:****:
cpe:2.3:a:f5:big-ip_application_security_manager:13.0.0:****:
cpe:2.3:a:f5:big-ip_domain_name_system:12.0.0:****:
cpe:2.3:a:f5:big-ip_domain_name_system:12.1.0:****:
cpe:2.3:a:f5:big-ip_domain_name_system:12.1.1:****:
cpe:2.3:a:f5:big-ip_domain_name_system:12.1.2:****:
cpe:2.3:a:f5:big-ip_domain_name_system:13.0.0:****:
cpe:2.3:a:f5:big-ip_domain_name_system:12.0.0:****:
cpe:2.3:a:f5:big-ip_domain_name_system:12.1.0:****:
cpe:2.3:a:f5:big-ip_domain_name_system:12.1.1:****:
cpe:2.3:a:f5:big-ip_domain_name_system:12.1.2:****:
cpe:2.3:a:f5:big-ip_domain_name_system:13.0.0:****:
cpe:2.3:a:f5:big-ip_link_controller:12.0.0:****:
cpe:2.3:a:f5:big-ip_link_controller:12.1.0:****:
cpe:2.3:a:f5:big-ip_link_controller:12.1.1:****:
cpe:2.3:a:f5:big-ip_link_controller:12.1.2:****:
cpe:2.3:a:f5:big-ip_link_controller:13.0.0:****:
cpe:2.3:a:f5:big-ip_link_controller:12.0.0:****:
cpe:2.3:a:f5:big-ip_link_controller:12.1.0:****:
cpe:2.3:a:f5:big-ip_link_controller:12.1.1:****:
cpe:2.3:a:f5:big-ip_link_controller:12.1.2:****:

cpe:2.3:a:f5:big-ip_link_controller:12.1.2:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_link_controller:13.0.0:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_local_traffic_manager:12.0.0:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_local_traffic_manager:12.1.0:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_local_traffic_manager:12.1.1:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_local_traffic_manager:12.1.2:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_local_traffic_manager:13.0.0:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_local_traffic_manager:12.0.0:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_local_traffic_manager:12.1.0:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_local_traffic_manager:12.1.1:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_local_traffic_manager:12.1.2:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_local_traffic_manager:13.0.0:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_policy_enforcement_manager:12.0.0:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_policy_enforcement_manager:12.1.0:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_policy_enforcement_manager:12.1.1:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_policy_enforcement_manager:12.1.2:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_policy_enforcement_manager:13.0.0:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_policy_enforcement_manager:12.0.0:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_policy_enforcement_manager:12.1.0:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_policy_enforcement_manager:12.1.1:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_policy_enforcement_manager:12.1.2:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_policy_enforcement_manager:13.0.0:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_websafe:12.0.0:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_websafe:12.1.0:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_websafe:12.1.1:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_websafe:12.1.2:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_websafe:13.0.0:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_websafe:12.0.0:*:*:*:*:*:
cpe:2.3:a:f5:big-ip_websafe:12.1.0:*:*:*:*:*:

cpe:2.3:a:f5:big-ip_websafe:12.1.1.*:*:*:*:*:
cpe:2.3:a:f5:big-ip_websafe:12.1.2.*:*:*:*:*:
cpe:2.3:a:f5:big-ip_websafe:13.0.0.*:*:*:*:*:

```
cpe:2.3:a:f5:big-ip_websafe:12.1.2.*.*.*.*.*:
```

```
cpe:2.3:a:f5:big-ip_websafe:13.0.0.*:*:*:*:*:
```

No vendor comments have been submitted for this CVE

[← 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