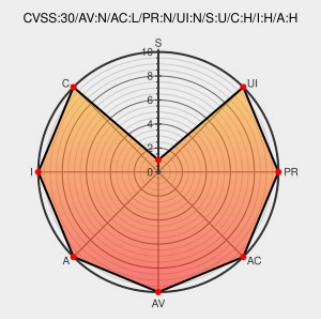
CVE-2015-8611

Published on: 01/12/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:14 PM UTC

CVE-2015-8611

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



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

BIG-IP LTM, AAM, AFM, Analytics, APM, ASM, DNS, Link Controller, and PEM 12.0.0 before HF1 on the 2000, 4000, 5000, 7000, and 10000 platforms do not properly sync passwords with the Always-On Management (AOM) subsystem, which might allow remote attackers to obtain login access to AOM via an (1) expired or (2) default password.

CVE-2015-8611 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

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: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
F5 BIG-IP Always-On Management Flaw Lets Remote Authenticated Users Access the Target System with Previous Passwords - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1034629

SOL05272632 - BIG-IP AOM password sync vulnerability CVE-2015-8611	Vendor Advisory support.f5.com text/html	CONFIRM support.f5.com/kb/en-us/solutions/public/k/05/sol05272632.html

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	12.0.0	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	12.0.0	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	12.0.0	All	All	All
Application	F5	Big-ip Analytics	12.0.0	All	All	All
Application	F5	Big-ip Analytics	12.0.0	All	All	All
Application	F5	Big-ip Application Acceleration Manager	12.0.0	All	All	All
Application	F5	Big-ip Application Acceleration Manager	12.0.0	All	All	All
Application	F5	Big-ip Application Security Manager	12.0.0	All	All	All
Application	F5	Big-ip Application Security Manager	12.0.0	All	All	All
Application	F5	Big-ip Domain Name System	12.0.0	All	All	All
Application	F5	Big-ip Domain Name System	12.0.0	All	All	All
Application	F5	Big-ip Link Controller	12.0.0	All	All	All
Application	F5	Big-ip Link Controller	12.0.0	All	All	All
Application	F5	Big-ip Local Traffic Manager	12.0.0	All	All	All
Application	F5	Big-ip Local Traffic Manager	12.0.0	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	12.0.0	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	12.0.0	All	All	All

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→