



CVE-2019-6646

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2019-6646
State	PUBLIC
Assigner	f5sirt@f5.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-09-04 18:15:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	On BIG-IP 11.5.2-11.6.4 and Enterprise Manager 3.1.1, REST users with guest privileges may be able to escalate their priv

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

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 Access Policy Manager	All	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 Advanced Firewall Manager	All	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 Analytics	All	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 Acceleration Manager	All	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 Application Security Manager	All	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 Domain Name System	All	All	All	All
Application	F5	Big-ip Edge Gateway	12.0.0	All	All	All
Application	F5	Big-ip Edge Gateway	12.0.0	All	All	All
Application	F5	Big-ip Edge Gateway	All	All	All	All
Application	F5	Big-ip Fraud Protection Service	12.0.0	All	All	All
Application	F5	Big-ip Fraud Protection Service	12.0.0	All	All	All
Application	F5	Big-ip Fraud Protection Service	All	All	All	All
Application	F5	Big-ip Global Traffic Manager	12.0.0	All	All	All
Application	F5	Big-ip Global Traffic Manager	12.0.0	All	All	All
Application	F5	Big-ip Global Traffic Manager	All	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 Link Controller	All	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 Local Traffic Manager	All	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
Application	F5	Big-ip Policy Enforcement Manager	All	All	All	All
Application	F5	Big-ip Webaccelerator	12.0.0	All	All	All
Application	F5	Big-ip Webaccelerator	12.0.0	All	All	All
Application	F5	Big-ip Webaccelerator	All	All	All	All
Application	F5	Enterprise Manager	3.1.1	All	All	All
Application	F5	Enterprise Manager	3.1.1	All	All	All

References

Reference	Source	Link	Tags
support.f5.com/csp/article/K53990093	MISC	support.f5.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#)