



CVE-2018-5511

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2018-5511
State	PUBLIC
Assigner	f5sirt@f5.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-04-13 13:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	On F5 BIG-IP 13.1.0-13.1.0.3 or 13.0.0, when authenticated administrative users execute commands in the Traffic Manage

Risk And Classification

Problem Types: CWE-470

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	F5	Big-ip Access Policy Manager	13.0.0	All	All	All
Application	F5	Big-ip Access Policy Manager	13.1.0	All	All	All
Application	F5	Big-ip Access Policy Manager	13.0.0	All	All	All
Application	F5	Big-ip Access Policy Manager	13.1.0	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	13.0.0	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	13.1.0	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	13.0.0	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	13.1.0	All	All	All
Application	F5	Big-ip Analytics	13.0.0	All	All	All
Application	F5	Big-ip Analytics	13.1.0	All	All	All
Application	F5	Big-ip Analytics	13.0.0	All	All	All
Application	F5	Big-ip Analytics	13.1.0	All	All	All
Application	F5	Big-ip Application Acceleration Manager	13.0.0	All	All	All
Application	F5	Big-ip Application Acceleration Manager	13.1.0	All	All	All
Application	F5	Big-ip Application Acceleration Manager	13.0.0	All	All	All
Application	F5	Big-ip Application Acceleration Manager	13.1.0	All	All	All
Application	F5	Big-ip Application Security Manager	13.0.0	All	All	All

Application	F5	Big-ip Application Security Manager	13.1.0	All	All	All
Application	F5	Big-ip Application Security Manager	13.0.0	All	All	All
Application	F5	Big-ip Application Security Manager	13.1.0	All	All	All
Application	F5	Big-ip Domain Name System	13.0.0	All	All	All
Application	F5	Big-ip Domain Name System	13.1.0	All	All	All
Application	F5	Big-ip Domain Name System	13.0.0	All	All	All
Application	F5	Big-ip Domain Name System	13.1.0	All	All	All
Application	F5	Big-ip Edge Gateway	13.0.0	All	All	All
Application	F5	Big-ip Edge Gateway	13.1.0	All	All	All
Application	F5	Big-ip Edge Gateway	13.0.0	All	All	All
Application	F5	Big-ip Edge Gateway	13.1.0	All	All	All
Application	F5	Big-ip Enterprise Manager	3.1.1	All	All	All
Application	F5	Big-ip Enterprise Manager	3.1.1	All	All	All
Application	F5	Big-ip Global Traffic Manager	13.0.0	All	All	All
Application	F5	Big-ip Global Traffic Manager	13.1.0	All	All	All
Application	F5	Big-ip Global Traffic Manager	13.0.0	All	All	All
Application	F5	Big-ip Global Traffic Manager	13.1.0	All	All	All
Application	F5	Big-ip Link Controller	13.0.0	All	All	All
Application	F5	Big-ip Link Controller	13.1.0	All	All	All
Application	F5	Big-ip Link Controller	13.0.0	All	All	All
Application	F5	Big-ip Link Controller	13.1.0	All	All	All
Application	F5	Big-ip Local Traffic Manager	13.0.0	All	All	All
Application	F5	Big-ip Local Traffic Manager	13.1.0	All	All	All
Application	F5	Big-ip Local Traffic Manager	13.0.0	All	All	All
Application	F5	Big-ip Local Traffic Manager	13.1.0	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	13.0.0	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	13.1.0	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	13.0.0	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	13.1.0	All	All	All
Application	F5	Big-ip Webaccelerator	13.0.0	All	All	All
Application	F5	Big-ip Webaccelerator	13.1.0	All	All	All
Application	F5	Big-ip Webaccelerator	13.0.0	All	All	All
Application	F5	Big-ip Webaccelerator	13.1.0	All	All	All
Application	F5	Big-ip Websafe	13.0.0	All	All	All
Application	F5	Big-ip Websafe	13.1.0	All	All	All

Application	F5	Big-ip Websafe	13.0.0	All	All	All
Application	F5	Big-ip Websafe	13.1.0	All	All	All
Operating System	Microsoft	Windows 10	All	All	All	All
Operating System	Microsoft	Windows 10	All	All	All	All
Application	Vmware	Workstation	14.1.5	All	All	All
Application	Vmware	Workstation	14.1.5	All	All	All
Application	Vmware	Workstation Player	15.0.2	All	All	All
Application	Vmware	Workstation Player	15.0.2	All	All	All

References

Reference

VMware Host VMX Process Impersonation Hijack Privilege Escalation ≈ Packet Storm

support.f5.com/csp/article/K30500703

VMware Workstation 14.1.5 / VMware Player 15.0.2 - Host VMX Process Impersonation Hijack Privilege Escalation - Windows local Exploit

CVE Program record

NVD vulnerability detail

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