



CVE-2020-5906

Published on: 07/01/2020 12:00:00 AM UTC

Last Modified on: 01/27/2023 04:38:00 PM UTC

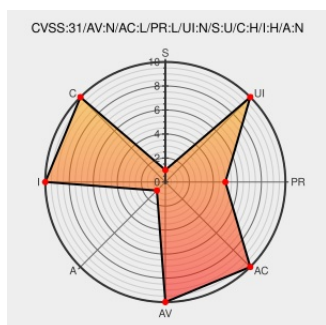
CVE-2020-5906

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

In versions 13.1.0-13.1.3.3, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2, the BIG-IP system does not properly enforce the access controls for the scp.blacklist files. This allows Admin and Resource Admin users with Secure Copy (SCP) protocol access to read and overwrite blacklisted files via SCP.

CVE-2020-5906 has been assigned by f5sirt@f5.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.1 - HIGH**

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

CVSS2 Score: **5.5 - MEDIUM**

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

CVE References

Description	Tags	Link
No Description Provided	Vendor Advisory support.f5.com text/html	MISC support.f5.com/csp/article/K82518062

VU#290915 - F5 BIG-IP contains multiple vulnerabilities including unauthenticated remote command execution

www.kb.cert.org

[text/html](#)

 CERT-VN VU#290915

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	All	All	All	All
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 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 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 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 Application Security Manager	All	All	All	All
Application	F5	Big-ip Domain Name System	All	All	All	All
Application	F5	Big-ip Domain Name System	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 Fraud Protection Service	All	All	All	All
Application	F5	Big-ip Global Traffic Manager	All	All	All	All
Application	F5	Big-ip Global Traffic Manager	All	All	All	All
Application	F5	Big-ip Global Traffic Manager	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 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 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 Policy Enforcement Manager	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_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_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_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_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_application_security_manager:*.*.*.*.*.*.*.*:						
cpe:2.3:a:f5:big-ip_domain_name_system:*.*.*.*.*.*.*.*:						
cpe:2.3:a:f5:big-ip_domain_name_system:*.*.*.*.*.*.*.*:						
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_fraud_protection_service:*.*.*.*.*.*.*.*:						
cpe:2.3:a:f5:big-ip_global_traffic_manager:*.*.*.*.*.*.*.*:						
cpe:2.3:a:f5:big-ip_global_traffic_manager:*.*.*.*.*.*.*.*:						

```
cpe:2.3:a:f5:big-ip_global_traffic_manager:*.:*:*:*:*:*.*
```

```
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 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_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 policy enforcement manager:*:*:*:*:*.*
```

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