

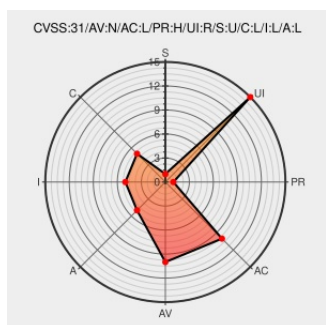


CVE-2020-5905

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

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-5905

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

In version 11.6.1-11.6.5.2 of the BIG-IP system Configuration utility Network > WCCP page, the system does not sanitize all user-provided data before display.

CVE-2020-5905 has been assigned by f5sirt@f5.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **4.3 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	LOW	LOW	LOW

CVSS2 Score: **6 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
No Description Provided	Vendor Advisory support.f5.com text/html	MISC support.f5.com/csp/article/K07051153
VU#290915 - F5 BIG-IP contains multiple vulnerabilities including	Third Party Advisory	CERT-VN VU#290915

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
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 Analytics	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 Domain Name System	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 Link Controller	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

```
cpe:2.3:a:f5:big-ip advanced firewall manager:*:*:*:*:*:*:
```

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

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

```
cpe:2.3:a:f5:big-ip global traffic manager:*:*:*:*:*:*:*:
```

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

No vendor comments have been submitted for this CVE

© 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](#)