



CVE-2018-5520

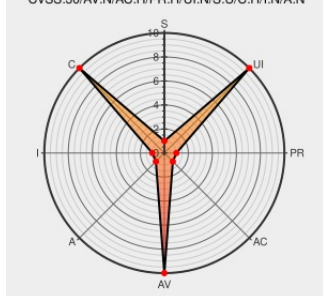
Published on: 05/02/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:45 PM UTC

CVE-2018-5520

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

CVSS:30/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N



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

On an F5 BIG-IP 13.0.0-13.1.0.5, 12.1.0-12.1.3.1, or 11.2.1-11.6.3.1 system configured in Appliance mode, the TMOS Shell (tmsh) may allow an administrative user to use the dig utility to gain unauthorized access to file system resources.

CVE-2018-5520 has been assigned by f5sirt@f5.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **F5 Networks, Inc. - BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, GTM, Link Controller, PEM, WebAccelerator, WebSafe)** version **13.0.0-13.1.0.5**

Affected Vendor/Software: **F5 Networks, Inc. - BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, GTM, Link Controller, PEM, WebAccelerator, WebSafe)** version **12.1.0-12.1.3.1**

Affected Vendor/Software: **F5 Networks, Inc. - BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, GTM, Link Controller, PEM, WebAccelerator, WebSafe)** version **11.2.1-11.6.3.1**

CVSS3 Score: **4.4 - MEDIUM**

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

CVSS2 Score: **3.5 - LOW**

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

CVE References		
Description	Tags	Link
No Description Provided	Vendor Advisory support.f5.com text/html	 CONFIRM support.f5.com/csp/article/K02043709
F5 BIG-IP Flaw in TMOS Shell Lets Remote Authenticated Administrative Users Obtain Potentially Sensitive Information - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	 SECTrack 1040798
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 Edge Gateway	All	All	All	All
Application	F5	Big-ip Edge Gateway	All	All	All	All
Application	F5	Big-ip Edge Gateway	All	All	All	All

Application	F5	Big-ip Edge Gateway	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
Application	F5	Big-ip Webaccelerator	All	All	All	All
Application	F5	Big-ip Webaccelerator	All	All	All	All
Application	F5	Big-ip Webaccelerator	All	All	All	All
Application	F5	Big-ip Websafe	All	All	All	All
Application	F5	Big-ip Websafe	All	All	All	All
Application	F5	Big-ip Websafe	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:t5: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_edge_gateway:*:*:*:*:*:*:*:
```

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

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

```
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:*.*.*.*.*.*.*.*
```

```
cpe:2.3:a:f5:big-ip webaccelerator:*:*:*:*:*:*:
```

```
cpe:2.3:a:f5:big-ip webaccelerator:*:*:*:*:*:*:
```

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

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

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

```
cpe:2.3:a:f5:big-ip websafe:*.~*~*~*~*~*~*~*~*~*
```

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](#)