



CVE-2019-6593

Published on: 02/26/2019 12:00:00 AM UTC

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

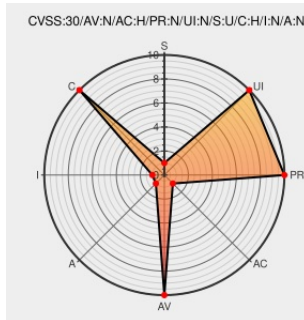
CVE-2019-6593

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

On BIG-IP 11.5.1-11.5.4, 11.6.1, and 12.1.0, a virtual server configured with a Client SSL profile may be vulnerable to a chosen ciphertext attack against CBC ciphers. When exploited, this may result in plaintext recovery of encrypted messages through a man-in-the-middle (MITM) attack, despite the attacker not having gained access to the server's private key itself. (CVE-2019-6593 also known as Zombie POODLE and GOLDENDOODLE.)

CVE-2019-6593 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, FPS, GTM, Link Controller, PEM, WebAccelerator)** version 11.5.1-11.5.4, 11.6.1, 12.1.0

CVSS3 Score: **5.9 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
-------------	------	------

Description

Tags

Link

No Description Provided

Vendor Advisory
support.f5.com
text/html

 CONFIRM support.f5.com/csp/article/K10065173

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	11.6.1	All	All	All
Application	F5	Big-ip Access Policy Manager	12.1.0	All	All	All
Application	F5	Big-ip Access Policy Manager	11.6.1	All	All	All
Application	F5	Big-ip Access Policy Manager	12.1.0	All	All	All
Application	F5	Big-ip Access Policy Manager	All	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	11.6.1	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	12.1.0	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	11.6.1	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	12.1.0	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	All	All	All	All
Application	F5	Big-ip Analytics	11.6.1	All	All	All
Application	F5	Big-ip Analytics	12.1.0	All	All	All
Application	F5	Big-ip Analytics	11.6.1	All	All	All
Application	F5	Big-ip Analytics	12.1.0	All	All	All
Application	F5	Big-ip Analytics	All	All	All	All
Application	F5	Big-ip Application Security Manager	11.6.1	All	All	All
Application	F5	Big-ip Application Security Manager	12.1.0	All	All	All
Application	F5	Big-ip Application Security Manager	11.6.1	All	All	All
Application	F5	Big-ip Application Security Manager	12.1.0	All	All	All
Application	F5	Big-ip Application Security Manager	All	All	All	All
Application	F5	Big-ip Domain Name System	11.6.1	All	All	All
Application	F5	Big-ip Domain Name System	12.1.0	All	All	All
Application	F5	Big-ip Domain Name System	11.6.1	All	All	All
Application	F5	Big-ip Domain Name System	12.1.0	All	All	All
Application	F5	Big-ip Domain Name System	All	All	All	All

Application	F5	Big-ip Edge Gateway	11.6.1	All	All	All
Application	F5	Big-ip Edge Gateway	12.1.0	All	All	All
Application	F5	Big-ip Edge Gateway	11.6.1	All	All	All
Application	F5	Big-ip Edge Gateway	12.1.0	All	All	All
Application	F5	Big-ip Edge Gateway	All	All	All	All
Application	F5	Big-ip Fraud Protection Service	11.6.1	All	All	All
Application	F5	Big-ip Fraud Protection Service	12.1.0	All	All	All
Application	F5	Big-ip Fraud Protection Service	11.6.1	All	All	All
Application	F5	Big-ip Fraud Protection Service	12.1.0	All	All	All
Application	F5	Big-ip Fraud Protection Service	All	All	All	All
Application	F5	Big-ip Global Traffic Manager	11.6.1	All	All	All
Application	F5	Big-ip Global Traffic Manager	12.1.0	All	All	All
Application	F5	Big-ip Global Traffic Manager	11.6.1	All	All	All
Application	F5	Big-ip Global Traffic Manager	12.1.0	All	All	All
Application	F5	Big-ip Global Traffic Manager	All	All	All	All
Application	F5	Big-ip Link Controller	11.6.1	All	All	All
Application	F5	Big-ip Link Controller	12.1.0	All	All	All
Application	F5	Big-ip Link Controller	11.6.1	All	All	All
Application	F5	Big-ip Link Controller	12.1.0	All	All	All
Application	F5	Big-ip Link Controller	All	All	All	All
Application	F5	Big-ip Local Traffic Manager	11.6.1	All	All	All
Application	F5	Big-ip Local Traffic Manager	12.1.0	All	All	All
Application	F5	Big-ip Local Traffic Manager	11.6.1	All	All	All
Application	F5	Big-ip Local Traffic Manager	12.1.0	All	All	All
Application	F5	Big-ip Local Traffic Manager	All	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	11.6.1	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	12.1.0	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	11.6.1	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	12.1.0	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	All	All	All	All
Application	F5	Big-ip Webaccelerator	11.6.1	All	All	All
Application	F5	Big-ip Webaccelerator	12.1.0	All	All	All
Application	F5	Big-ip Webaccelerator	11.6.1	All	All	All
Application	F5	Big-ip Webaccelerator	12.1.0	All	All	All
Application	F5	Big-ip Webaccelerator	All	All	All	All

```
cpe:2.3:a:f5:big-ip_access_policy_manager:11.6.1:*:*:*:*:*:
```

```
cpe:2.3:a:f5:big-ip_access_policy_manager:12.1.0:*:*:*:*:*:
```

```
cpe:2.3:a:f5:big-ip_access_policy_manager:11.6.1:*:*:*:*:*:
```

```
cpe:2.3:a:f5:big-ip_access_policy_manager:12.1.0:*:*:*:*:*:
```

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

```
cpe:2.3:a:f5:big-ip_advanced_firewall_manager:11.6.1:::*:*:*:*:*:
```

```
cpe:2.3:a:f5:big-ip_advanced_firewall_manager:12.1.0:*:*:*:*:*:
```

```
cpe:2.3:a:f5:big-ip_advanced_firewall_manager:11.6.1:*:*:*:*:*:
```

```
cpe:2.3:a:f5:big-ip_advanced_firewall_manager:12.1.0:::*:*:*:*:
```

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

```
cpe:2.3:a:f5:big-ip_analytics:11.6.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:f5:big-ip_analytics:12.1.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:f5:big-ip_analytics:11.6.1:::~::~:
```

```
cpe:2.3:a:f5:big-ip_analytics:12.1.0:*:*:*:*:*:*:
```

cpe:2.3:a:f5:big-ip_analytics:*:*:*:*:*:*:*:

```
cpe:2.3:a:f5:big-ip_application_security_manager:11.6.1:*:*:*:*:*:
```

```
cpe:2.3:a:f5:big-ip_application_security_manager:12.1.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:f5:big-ip_application_security_manager:11.6.1:*:*:*:*:*:
```

```
cpe:2.3:a:f5:big-ip_application_security_manager:12.1.0:*:*:*:*:*:
```

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

```
cpe:2.3:a:f5:big-ip_domain_name_system:11.6.1.*:*:*:*:*:
```

```
cpe:2.3:a:f5:big-ip_domain_name_system:12.1.0:*:*:*:*:*:
```

```
cpe:2.3:a:f5:big-ip_domain_name_system:11.6.1.*:*:*:*:*:
```

```
cpe:2.3:a:f5:big-ip_domain_name_system:12.1.0:*:*:*:*:*:
```

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

```
cpe:2.3:a:f5:big-ip_edge_gateway:11.6.1:::*:*:*:*:
```

```
cpe:2.3:a:f5:big-ip_edge_gateway:12.1.0:*:*:*:*:*:
```

```
cpe:2.3:a:f5:big-ip_edge_gateway:11.6.1:*:*:*:*:*:
```

```
cpe:2.3:a:f5:big-ip_edge_gateway:12.1.0:*:*:*:*:*:
```

cpe:2.3:a:f5:big-ip_edge_gateway:*****:
cpe:2.3:a:f5:big-ip_fraud_protection_service:11.6.1:*****:
cpe:2.3:a:f5:big-ip_fraud_protection_service:12.1.0:*****:
cpe:2.3:a:f5:big-ip_fraud_protection_service:11.6.1:*****:
cpe:2.3:a:f5:big-ip_fraud_protection_service:12.1.0:*****:
cpe:2.3:a:f5:big-ip_fraud_protection_service:*****:
cpe:2.3:a:f5:big-ip_global_traffic_manager:11.6.1:*****:
cpe:2.3:a:f5:big-ip_global_traffic_manager:12.1.0:*****:
cpe:2.3:a:f5:big-ip_global_traffic_manager:11.6.1:*****:
cpe:2.3:a:f5:big-ip_global_traffic_manager:12.1.0:*****:
cpe:2.3:a:f5:big-ip_global_traffic_manager:*****:
cpe:2.3:a:f5:big-ip_link_controller:11.6.1:*****:
cpe:2.3:a:f5:big-ip_link_controller:12.1.0:*****:
cpe:2.3:a:f5:big-ip_link_controller:11.6.1:*****:
cpe:2.3:a:f5:big-ip_link_controller:12.1.0:*****:
cpe:2.3:a:f5:big-ip_link_controller:*****:
cpe:2.3:a:f5:big-ip_local_traffic_manager:11.6.1:*****:
cpe:2.3:a:f5:big-ip_local_traffic_manager:12.1.0:*****:
cpe:2.3:a:f5:big-ip_local_traffic_manager:11.6.1:*****:
cpe:2.3:a:f5:big-ip_local_traffic_manager:12.1.0:*****:
cpe:2.3:a:f5:big-ip_local_traffic_manager:*****:
cpe:2.3:a:f5:big-ip_policy_enforcement_manager:11.6.1:*****:
cpe:2.3:a:f5:big-ip_policy_enforcement_manager:12.1.0:*****:
cpe:2.3:a:f5:big-ip_policy_enforcement_manager:11.6.1:*****:
cpe:2.3:a:f5:big-ip_policy_enforcement_manager:12.1.0:*****:
cpe:2.3:a:f5:big-ip_policy_enforcement_manager:*****:
cpe:2.3:a:f5:big-ip_webaccelerator:11.6.1:*****:
cpe:2.3:a:f5:big-ip_webaccelerator:12.1.0:*****:

cpe:2.3:a:f5:big-ip_webaccelerator:11.6.1:*****:	
cpe:2.3:a:f5:big-ip_webaccelerator:12.1.0:*****:	
cpe:2.3:a:f5:big-ip_webaccelerator:*****:	
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](#)