



# CVE-2022-34851

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

## Summary

<b>CVE</b>	CVE-2022-34851
<b>State</b>	PUBLIC
<b>Assigner</b>	f5sirt@f5.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-08-04 18:15:00 UTC
<b>Updated</b>	2022-08-10 18:09:00 UTC
<b>Description</b>	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all ver

## Risk And Classification

### Problem Types: CWE-20

## NVD Known Affected Configurations (CPE 2.3)

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	17.0.0	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	17.0.0	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	17.0.0	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	17.0.0	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	17.0.0	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	17.0.0	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	17.0.0	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	17.0.0	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	17.0.0	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	17.0.0	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	17.0.0	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	All	All	All	All
Application	F5	Big-iq Centralized Management	All	All	All	All

## References

Reference	Source	Link	Tags
support.f5.com/csp/article/K50310001	MISC	<a href="https://support.f5.com">support.f5.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

## Vendor Comments And Credit

### Discovery Credit

**LEGACY:** F5 acknowledges the KITRI BOB Team for bringing this issue to our attention and following the highest standards of coordinated disclosure. KITRI BOB Team: Jeong Su Hwan, Kim Dong Jun, Jung Min Woo, Jang Min Ki, Lee Jung Woo, Heo Seung Hwan

## Legacy QID Mappings

**376794** F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) Big-ip and Big-iq Icontrol Simple Object Access Protocol (SOAP) Vulnerability cve-2022-34851 (K50310001)

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](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)