



CVE-2023-43485

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2023-43485 |
| State | PUBLIC |
| Assigner | f5sirt@f5.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2023-10-10 13:15:00 UTC |
| Updated | 2023-10-17 20:31:00 UTC |
| Description | When TACACS+ audit forwarding is configured on BIG-IP or BIG-IQ system, sharedsecret is logged in plaintext in the audit |

Risk And Classification

Problem Types: CWE-532

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 | 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 Advanced Web Application Firewall | All | All | All | All |
| Application | F5 | Big-ip Advanced Web Application Firewall | All | All | All | All |
| Application | F5 | Big-ip Advanced Web Application Firewall | 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 Application Visibility And Reporting | All | All | All | All |
| Application | F5 | Big-ip Application Visibility And Reporting | All | All | All | All |
| Application | F5 | Big-ip Application Visibility And Reporting | All | All | All | All |
| Application | F5 | Big-ip Carrier-grade Nat | All | All | All | All |
| Application | F5 | Big-ip Carrier-grade Nat | All | All | All | All |
| Application | F5 | Big-ip Carrier-grade Nat | All | All | All | All |
| Application | F5 | Big-ip Ddos Hybrid Defender | All | All | All | All |
| Application | F5 | Big-ip Ddos Hybrid Defender | All | All | All | All |
| Application | F5 | Big-ip Ddos Hybrid Defender | 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 |
| Application | F5 | Big-ip Ssl Orchestrator | All | All | All | All |
| Application | F5 | Big-ip Ssl Orchestrator | All | All | All | All |
| Application | F5 | Big-ip Ssl Orchestrator | 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 |
| Application | F5 | Big-iq Centralized Management | All | All | All | All |

References

| Reference | Source | Link | Tags |
|--------------------------|---------|---|---------------------|
| myF5 | MISC | my.f5.com | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

379308 F5 BIG-IP Audit Log Vulnerability (K06110200)

© [CVE.report](https://cve.report) 2026 |

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

CVE.report and Source URL Uptime Status status.cve.report