



F5 BIG-IP Missing Authentication Vulnerability

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

Summary

CVE	CVE-2022-1388
State	PUBLIC
Assigner	f5sirt@f5.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-05-05 17:15:00 UTC
Updated	2023-11-02 01:54:00 UTC
Description	On F5 BIG-IP 16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x ver

Risk And Classification

EPSS: 0.944560000 probability, percentile 0.999930000 (date 2026-05-12)

CISA KEV: Listed on 2022-05-10; due 2022-05-31; ransomware use Known

Problem Types: CWE-306

CISA Known Exploited Vulnerability

Vendor	F5
Product	BIG-IP
Name	F5 BIG-IP Missing Authentication Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2022-1388

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 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 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

References						
Reference		Source	Link		Tags	
F5 BIG-IP iControl Remote Code Execution ≈ Packet Storm		MISC	packetstormsecurity.com			
F5 BIG-IP Remote Code Execution ≈ Packet Storm		MISC	packetstormsecurity.com			
CVE-2022-1388: F5 vulnerability exploited in 2022		MISC	www.secpod.com			
support.f5.com/csp/article/K23605346		MISC	support.f5.com			
F5 BIG-IP 16.0.x Remote Code Execution ≈ Packet Storm		MISC	packetstormsecurity.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

[150511](#) F5 BIG-IP iControl REST Remote Code Execution (RCE) Vulnerability (CVE-2022-1388)

[376577](#) F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) iControl REST Vulnerability (K23605346)

[730489](#) F5 BIG-IP iControl REST Remote Code Execution (RCE) Vulnerability (K23605346) (Unauthenticated Check)

© [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://cve.mitre.org). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

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