

CVE-2022-1388

F5 BIG-IP Missing Authentication Vulnerability

Exigent CISA KEV since May 10, 2022 Actively exploited Ransomware use known Public exploit module (Metasploit)

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 versions prior to 13.1.5, and all 12.1.x and 11.6.x versions, undisclosed requests may bypass iControl REST authentication. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated

EVRS 94 /100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.999 99.98th percentile · FIRST	CISA DEADLINE May 31, 2022 KEV since 2022 · listed over a year
--	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☒ Ransomware	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.999 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions · 3 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
big-ip access policy manager	≥ 11.6.1 ≤ 11.6.5 ≥ 12.1.0 ≤ 12.1.6 ≥ 13.1.0 < 13.1.5 ≥ 14.1.0 < 14.1.4.6 ≥ 15.1.0 < 15.1.5.1 ≥ 16.1.0 < 16.1.2.2	after 11.6.5 · after 12.1.6 · 13.1.5 · 14.1.4.6 · 15.1.5.1 · 16.1.2.2	NVD
big-ip advanced firewall manager	≥ 11.6.1 ≤ 11.6.5 ≥ 12.1.0 ≤ 12.1.6 ≥ 13.1.0 < 13.1.5 ≥ 14.1.0 < 14.1.4.6 ≥ 15.1.0 < 15.1.5.1 ≥ 16.1.0 < 16.1.2.2	no fixed version listed	NVD
big-ip analytics	≥ 11.6.1 ≤ 11.6.5 ≥ 12.1.0 ≤ 12.1.6 ≥ 13.1.0 < 13.1.5 ≥ 14.1.0 < 14.1.4.6 ≥ 15.1.0 < 15.1.5.1 ≥ 16.1.0 < 16.1.2.2	no fixed version listed	NVD

PACKAGE	AFFECTED	FIXED IN	SOURCE
big-ip application acceleration manager	$\geq 11.6.1 \leq 11.6.5$ $\geq 12.1.0 \leq 12.1.6$ $\geq 13.1.0 < 13.1.5$ $\geq 14.1.0 < 14.1.4.6$ $\geq 15.1.0 < 15.1.5.1$ $\geq 16.1.0 < 16.1.2.2$	no fixed version listed	NVD
big-ip application security manager	$\geq 11.6.1 \leq 11.6.5$ $\geq 12.1.0 \leq 12.1.6$ $\geq 13.1.0 < 13.1.5$ $\geq 14.1.0 < 14.1.4.6$ $\geq 15.1.0 < 15.1.5.1$ $\geq 16.1.0 < 16.1.2.2$	no fixed version listed	NVD
big-ip domain name system	$\geq 11.6.1 \leq 11.6.5$ $\geq 12.1.0 \leq 12.1.6$ $\geq 13.1.0 < 13.1.5$ $\geq 14.1.0 < 14.1.4.6$ $\geq 15.1.0 < 15.1.5.1$ $\geq 16.1.0 < 16.1.2.2$	no fixed version listed	NVD
big-ip fraud protection service	$\geq 11.6.1 \leq 11.6.5$ $\geq 12.1.0 \leq 12.1.6$ $\geq 13.1.0 < 13.1.5$ $\geq 14.1.0 < 14.1.4.6$ $\geq 15.1.0 < 15.1.5.1$ $\geq 16.1.0 < 16.1.2.2$	no fixed version listed	NVD
big-ip global traffic manager	$\geq 11.6.1 \leq 11.6.5$ $\geq 12.1.0 \leq 12.1.6$ $\geq 13.1.0 < 13.1.5$ $\geq 14.1.0 < 14.1.4.6$ $\geq 15.1.0 < 15.1.5.1$ $\geq 16.1.0 < 16.1.2.2$	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-mrph-rvc3-cv97
NVD nvd.nist.gov/vuln/detail/CVE-2022-1388

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2022-24705

Additional guidance support.f5.com/csp/article/K23605346
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2022-1388

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.