

CVE-2023-46747

F5 BIG-IP Configuration Utility Authentication Bypass Vulnerability

Exigent

CISA KEV since Oct 31, 2023

Actively exploited

Ransomware use known

Public exploit module (Metasploit)

Undisclosed requests may bypass configuration utility authentication, allowing an attacker with network access to the BIG-IP system through the management port and/or self IP addresses to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated

EVRS 93/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.965 99.88th percentile · FIRST	CISA DEADLINE Nov 21, 2023 KEV since 2023 · 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	0.965 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 mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
Basis: CISA KEV required action

Affected and fixed versions · 12 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
big-ip access policy manager	$\geq 13.1.0 \leq 13.1.5$ $\geq 14.1.0 \leq 14.1.5$ $\geq 15.1.0 \leq 15.1.10$ $\geq 16.1.0 \leq 16.1.4$ $\geq 17.1.0 \leq 17.1.1$	after 13.1.5 · after 14.1.5 · after 15.1.10 · after 16.1.4 · after 17.1.1	NVD
big-ip advanced firewall manager	$\geq 13.1.0 \leq 13.1.5$ $\geq 14.1.0 \leq 14.1.5$ $\geq 15.1.0 \leq 15.1.10$ $\geq 16.1.0 \leq 16.1.4$ $\geq 17.1.0 \leq 17.1.1$	after 13.1.5	NVD
big-ip advanced web application firewall	$\geq 13.1.0 \leq 13.1.5$ $\geq 14.1.0 \leq 14.1.5$ $\geq 15.1.0 \leq 15.1.10$ $\geq 16.1.0 \leq 16.1.4$ $\geq 17.1.0 \leq 17.1.1$	no fixed version listed	NVD
big-ip carrier-grade nat	$\geq 13.1.0 \leq 13.1.5$ $\geq 14.1.0 \leq 14.1.5$ $\geq 15.1.0 \leq 15.1.10$ $\geq 16.1.0 \leq 16.1.4$ $\geq 17.1.0 \leq 17.1.1$	no fixed version listed	NVD

PACKAGE	AFFECTED	FIXED IN	SOURCE
big-ip ddos hybrid defender	≥ 13.1.0 ≤ 13.1.5	no fixed version listed	NVD
	≥ 14.1.0 ≤ 14.1.5		
	≥ 15.1.0 ≤ 15.1.10		
	≥ 16.1.0 ≤ 16.1.4		
	≥ 17.1.0 ≤ 17.1.1		
big-ip ssl orchestrator	≥ 13.1.0 ≤ 13.1.5	no fixed version listed	NVD
	≥ 14.1.0 ≤ 14.1.5		
	≥ 15.1.0 ≤ 15.1.10		
	≥ 16.1.0 ≤ 16.1.4		
	≥ 17.1.0 ≤ 17.1.1		
big-ip domain name system	≥ 13.1.0 ≤ 13.1.5	no fixed version listed	NVD
	≥ 14.1.0 ≤ 14.1.5		
	≥ 15.1.0 ≤ 15.1.10		
	≥ 16.1.0 ≤ 16.1.4		
	≥ 17.1.0 ≤ 17.1.1		
big-ip local traffic manager	≥ 13.1.0 ≤ 13.1.5	no fixed version listed	NVD
	≥ 14.1.0 ≤ 14.1.5		
	≥ 15.1.0 ≤ 15.1.10		
	≥ 16.1.0 ≤ 16.1.4		
	≥ 17.1.0 ≤ 17.1.1		

Sources

Vendor guidance github.com/advisories/GHSA-pq6p-fc96-wc5w
NVD nvd.nist.gov/vuln/detail/CVE-2023-46747

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2023-50916

Additional guidance my.f5.com/manage/s/article/K000137353
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2023-46747

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