

CVE-2020-5902

F5 BIG-IP Traffic Management User Interface (TMUI) Remote Code Execution Vulnerability

Exigent CISA KEV since Nov 3, 2021 Actively exploited Ransomware use known Public exploit module (Metasploit)

In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages.

EVRS 94 /100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.999 99.99th percentile · FIRST	CISA DEADLINE May 3, 2022 KEV since 2021 · 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 · 6 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
big-ip access policy manager	≥ 11.6.1 < 11.6.5.2 ≥ 12.1.0 < 12.1.5.2 ≥ 13.1.0 < 13.1.3.4 ≥ 14.1.0 < 14.1.2.6 ≥ 15.0.0 ≤ 15.0.1.4 ≥ 15.1.0 < 15.1.0.4	11.6.5.2 · 12.1.5.2 · 13.1.3.4 · 14.1.2.6 · after 15.0.1.4 · 15.1.0.4	NVD
big-ip advanced firewall manager	≥ 11.6.1 < 11.6.5.2 ≥ 12.1.0 < 12.1.5.2 ≥ 13.1.0 < 13.1.3.4 ≥ 14.1.0 < 14.1.2.6 ≥ 15.0.0 < 15.0.1.4 ≥ 15.1.0 < 15.1.0.4	no fixed version listed	NVD
big-ip advanced web application firewall	≥ 11.6.1 < 11.6.5.2 ≥ 12.1.0 < 12.1.5.2 ≥ 13.1.0 < 13.1.3.4 ≥ 14.1.0 < 14.1.2.6 ≥ 15.0.0 < 15.0.1.4 ≥ 15.1.0 < 15.1.0.4	no fixed version listed	NVD

PACKAGE	AFFECTED	FIXED IN	SOURCE
big-ip analytics	$\geq 11.6.1 < 11.6.5.2$ $\geq 12.1.0 < 12.1.5.2$ $\geq 13.1.0 < 13.1.3.4$ $\geq 14.1.0 < 14.1.2.6$ $\geq 15.0.0 < 15.0.1.4$ $\geq 15.1.0 < 15.1.0.4$	no fixed version listed	NVD
big-ip application acceleration manager	$\geq 11.6.1 < 11.6.5.2$ $\geq 12.1.0 < 12.1.5.2$ $\geq 13.1.0 < 13.1.3.4$ $\geq 14.1.0 < 14.1.2.6$ $\geq 15.0.0 < 15.0.1.4$ $\geq 15.1.0 < 15.1.0.4$	no fixed version listed	NVD
big-ip application security manager	$\geq 11.6.1 < 11.6.5.2$ $\geq 12.1.0 < 12.1.5.2$ $\geq 13.1.0 < 13.1.3.4$ $\geq 14.1.0 < 14.1.2.6$ $\geq 15.0.0 < 15.0.1.4$ $\geq 15.1.0 < 15.1.0.4$	no fixed version listed	NVD
big-ip ddos hybrid defender	$\geq 11.6.1 < 11.6.5.2$ $\geq 12.1.0 < 12.1.5.2$ $\geq 13.1.0 < 13.1.3.4$ $\geq 14.1.0 < 14.1.2.6$ $\geq 15.0.0 < 15.0.1.4$ $\geq 15.1.0 < 15.1.0.4$	no fixed version listed	NVD
big-ip domain name system	$\geq 11.6.1 < 11.6.5.2$ $\geq 12.1.0 < 12.1.5.2$ $\geq 13.1.0 < 13.1.3.4$ $\geq 14.1.0 < 14.1.2.6$ $\geq 15.0.0 < 15.0.1.4$ $\geq 15.1.0 < 15.1.0.4$	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-2859-2hr6-f86v
NVD nvd.nist.gov/vuln/detail/CVE-2020-5902

Additional guidance support.f5.com/csp/article/K52145254
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2020-5902

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2020-27056

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