

CVE-2021-22991

F5 BIG-IP Traffic Management Microkernel Buffer Overflow

CISA KEV since Jan 18, 2022

Actively exploited

On BIG-IP versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.2.1, 14.1.x before 14.1.4, 13.1.x before 13.1.3.6, and 12.1.x before 12.1.5.3, undisclosed requests to a virtual server may be incorrectly handled by the Traffic Management Microkernel (TMM) URI normalization, which may trigger a buffer overflow, resulting in a DoS attack. In certain situations, it may theoretically allow bypass of URL based access control or remote code execution (RCE). Note: Software versions which have reached End of Software Development (EoSd) are not evaluated.

EVRS 77/₁₀₀ Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.611 99.16th percentile · FIRST	CISA DEADLINE Feb 1, 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	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.611 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle 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	≥ 12.1.0 < 12.1.5.3 ≥ 13.1.0 < 13.1.3.6 ≥ 14.1.0 < 14.1.4 ≥ 15.1.0 < 15.1.2.1 ≥ 16.0.0 < 16.0.1.1	12.1.5.3 · 13.1.3.6 · 14.1.4 · 15.1.2.1 · 16.0.1.1	NVD
big-ip advanced firewall manager	≥ 12.1.0 < 12.1.5.3 ≥ 13.1.0 < 13.1.3.6 ≥ 14.1.0 < 14.1.4 ≥ 15.1.0 < 15.1.2.1 ≥ 16.0.0 < 16.0.1.1	12.1.5.3	NVD
big-ip advanced web application firewall	≥ 12.1.0 < 12.1.5.3 ≥ 13.1.0 < 13.1.3.6 ≥ 14.1.0 < 14.1.4 ≥ 15.1.0 < 15.1.2.1 ≥ 16.0.0 < 16.0.1.1	no fixed version listed	NVD
big-ip analytics	≥ 12.1.0 < 12.1.5.3 ≥ 13.1.0 < 13.1.3.6 ≥ 14.1.0 < 14.1.4 ≥ 15.1.0 < 15.1.2.1 ≥ 16.0.0 < 16.0.1.1	no fixed version listed	NVD

PACKAGE	AFFECTED	FIXED IN	SOURCE
big-ip application acceleration manager	$\geq 12.1.0 < 12.1.5.3$ $\geq 13.1.0 < 13.1.3.6$ $\geq 14.1.0 < 14.1.4$ $\geq 15.1.0 < 15.1.2.1$ $\geq 16.0.0 < 16.0.1.1$	no fixed version listed	NVD
big-ip application security manager	$\geq 12.1.0 < 12.1.5.3$ $\geq 13.1.0 < 13.1.3.6$ $\geq 14.1.0 < 14.1.4$ $\geq 15.1.0 < 15.1.2.1$ $\geq 16.0.0 < 16.0.1.1$	no fixed version listed	NVD
big-ip ddos hybrid defender	$\geq 12.1.0 < 12.1.5.3$ $\geq 13.1.0 < 13.1.3.6$ $\geq 14.1.0 < 14.1.4$ $\geq 15.1.0 < 15.1.2.1$ $\geq 16.0.0 < 16.0.1.1$	no fixed version listed	NVD
big-ip domain name system	$\geq 12.1.0 < 12.1.5.3$ $\geq 13.1.0 < 13.1.3.6$ $\geq 14.1.0 < 14.1.4$ $\geq 15.1.0 < 15.1.2.1$ $\geq 16.0.0 < 16.0.1.1$	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-6w8r-pjm3-q7x7
NVD nvd.nist.gov/vuln/detail/CVE-2021-22991

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2021-10109

Additional guidance support.f5.com/csp/article/K56715231
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2021-22991

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