

CVE-2021-27102

Accellion FTA OS Command Injection Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

Ransomware use known

Accellion FTA 9_12_411 and earlier is affected by OS command execution via a local web service call. The fixed version is FTA_9_12_416 and later.

EVRS 75/₁₀₀ Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.037 89.6th percentile · FIRST	CISA DEADLINE Nov 17, 2021 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	0.037 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.8	☐ 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

PACKAGE	AFFECTED	FIXED IN	SOURCE
fta	≤ 9_12_411	after 9_12_411	NVD

Sources

Vendor guidance github.com/advisories/GHSA-vcwv-2759-43q3
NVD nvd.nist.gov/vuln/detail/CVE-2021-27102

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2021-13872

Additional guidance accellion.com/products/fta/
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2021-27102

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