

CVE-2018-19410

Paessler PRTG Network Monitor Local File Inclusion Vulnerability

Exigent

CISA KEV since Feb 4, 2025

Actively exploited

PRTG Network Monitor before 18.2.40.1683 allows remote unauthenticated attackers to create users with read-write privileges (including administrator). A remote unauthenticated user can craft an HTTP request and override attributes of the 'include' directive in /public/login.htm and perform a Local File Inclusion attack, by including /api/addusers and executing it. By providing the 'id' and 'users' parameters, an unauthenticated attacker can create a user with read-write privileges (including administrator).

EVRS 88/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.979 99.91st percentile · FIRST	CISA DEADLINE Feb 25, 2025 KEV since 2025 · 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	Added to CISA KEV within the last two years
☒ EPSS	0.979 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

PACKAGE	AFFECTED	FIXED IN	SOURCE
prtg network monitor	< 18.2.40.1683	18.2.40.1683	NVD

Sources

Vendor guidance github.com/advisories/GHSA-pm93-g4gf-j42f
NVD nvd.nist.gov/vuln/detail/CVE-2018-19410
ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2018-11103

paessler.com paessler.com/prtg/history/prtg-18#18.2.41.1652
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2018-19410

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