

CVE-2019-18935

Progress Telerik UI for ASP.NET AJAX Deserialization of Untrusted Data Vulnerability

Exigent

CISA KEV since Nov 3, 2021

Actively exploited

Ransomware use known

Public exploit module (Metasploit)

Progress Telerik UI for ASP.NET AJAX through 2019.3.1023 contains a .NET deserialization vulnerability in the RadAsyncUpload function. This is exploitable when the encryption keys are known due to the presence of CVE-2017-11317 or CVE-2017-11357, or other means. Exploitation can result in remote code execution. (As of 2020.1.114, a default setting prevents the exploit. In 2019.3.1023, but not earlier versions, a non-default setting can prevent exploitation.)

EVRS

94/100

Immediate priority

CVSS V3.1

9.8

Critical · NVD

EPSS

0.997

99.95th 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	0.997 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

PACKAGE	AFFECTED	FIXED IN	SOURCE
ui for asp.net ajax	≥ 2011.1.315 ≤ 2020.1.114	after 2020.1.114	NVD

Sources

Vendor guidance	telerik.com/support/kb/aspnet-ajax/details/allows-javascriptserializer-deserialization	NVD	nvd.nist.gov/vuln/detail/CVE-2019-18935
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2019-8608
Current data	evulnable.com/vulnerability-management/cve/CVE-2019-18935		

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