

CVE-2017-9248

Progress Telerik UI for ASP.NET AJAX and Sitefinity Cryptographic Weakness Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

Telerik.Web.UI.dll in Progress Telerik UI for ASP.NET AJAX before R2 2017 SP1 and Sitefinity before 10.0.6412.0 does not properly protect Telerik.Web.UI.DialogParametersEncryptionKey or the MachineKey, which makes it easier for remote attackers to defeat cryptographic protection mechanisms, leading to a MachineKey leak, arbitrary file uploads or downloads, XSS, or ASP.NET ViewState compromise.

EVRS 80 / ₁₀₀ Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.751 99.51st 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	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.751 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

PACKAGE	AFFECTED	FIXED IN	SOURCE
sitefinity	< 10.0.6412.0	10.0.6412.0	NVD
ui for asp.net ajax	≤ 2017.2.503	after 2017.2.503	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-mfqq-q5rf-3hvf	NVD	nvd.nist.gov/vuln/detail/CVE-2017-9248
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2017-18184
Current data	evulnable.com/vulnerability-management/cve/CVE-2017-9248		

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