

CVE-2021-42237

Sitecore XP Remote Command Execution Vulnerability

Exigent

CISA KEV since Mar 25, 2022

Actively exploited

Ransomware use known

Public exploit module (Metasploit)

Sitecore XP 7.5 Initial Release to Sitecore XP 8.2 Update-7 is vulnerable to an insecure deserialization attack where it is possible to achieve remote command execution on the machine. No authentication or special configuration is required to exploit this vulnerability.

EVRS 93 /100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.976 99.9th percentile · FIRST	CISA DEADLINE Apr 15, 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	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.976 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
experience platform	7.5 8.0 8.1 8.2	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-j3x5-fr4h-9v7v**Additional guidance** support.sitecore.com/kb?id=kb_article_view&sysparm_article=KB1000776**NVD** nvd.nist.gov/vuln/detail/CVE-2021-42237**CISA KEV** cisa.gov/known-exploited-vulnerabilities-catalog**ENISA EUVD** euvd.enisa.europa.eu/vulnerability/EUVD-2021-29215**Current data** evulnable.com/vulnerability-management/cve/CVE-2021-42237

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