

CVE-2021-39144

XStream Remote Code Execution Vulnerability

CISA KEV since Mar 10, 2023

Actively exploited

Public exploit module (Metasploit)

XStream is a simple library to serialize objects to XML and back again. In affected versions this vulnerability may allow a remote attacker has sufficient rights to execute commands of the host only by manipulating the processed input stream. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. XStream 1.4.18 uses no longer a blacklist by default, since it cannot be secured for general purpose.

EVRS 85/100 Immediate priority	CVSS V3.1 8.5 High · NVD	EPSS 0.981 99.91st percentile · FIRST	CISA DEADLINE Mar 31, 2023 KEV since 2023 · 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	0.981 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.5	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch Immediately Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions · 7 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
com.thoughtworks.xstream:xstream	1.4.18	1.4.18	GitHub
xstream	< 1.4.18	no fixed version listed	NVD
snapmanager	—	no fixed version listed	NVD
business activity monitoring	12.2.1.4.0	no fixed version listed	NVD
commerce guided search	11.3.2	no fixed version listed	NVD
communications billing and revenue management elastic charging engine	11.3 12.0	no fixed version listed	NVD
communications cloud native core automated test suite	1.9.0	no fixed version listed	NVD
communications cloud native core binding support function	1.10.0	no fixed version listed	NVD
communications cloud native core policy	1.14.0	no fixed version listed	NVD

Sources

Vendor guidance	oracle.com/security-alerts/cpuapr2022.html	Additional guidance	github.com/x-stream/xstream/security/advisories/GHSA-j9h8-phrw-h4fh
vmware.com	vmware.com/security/advisories/VMSA-2022-0027.html , https://x-stream.github.io/CVE-2021-39144.html	NVD	nvd.nist.gov/vuln/detail/CVE-2021-39144
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	GitHub advisory	github.com/advisories/GHSA-j9h8-phrw-h4fh
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2021-1771	Current data	evulnable.com/vulnerability-management/cve/CVE-2021-39144

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