



CVE-2021-39149

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2021-39149
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-23 18:15:00 UTC
Updated	2023-11-07 03:37:00 UTC
Description	XStream is a simple library to serialize objects to XML and back again. In affected versions this vulnerability may allow a re

Risk And Classification

Problem Types: CWE-502 | CWE-434

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update
Operating System	Debian	Debian Linux	10.0	All
Operating System	Debian	Debian Linux	11.0	All
Operating System	Debian	Debian Linux	9.0	All
Operating System	Fedoraproject	Fedora	33	All
Operating System	Fedoraproject	Fedora	34	All
Operating System	Fedoraproject	Fedora	35	All
Application	Netapp	Snapmanager	-	All
Application	Netapp	Snapmanager	-	All
Application	Oracle	Business Activity Monitoring	12.2.1.4.0	All
Application	Oracle	Commerce Guided Search	11.3.2	All
Application	Oracle	Communications Billing And Revenue Management Elastic Charging Engine	11.3	All
Application	Oracle	Communications Billing And Revenue Management Elastic Charging Engine	12.0	All
Application	Oracle	Communications Cloud Native Core Automated Test Suite	1.9.0	All
Application	Oracle	Communications Cloud Native Core Binding Support Function	1.10.0	All
Application	Oracle	Communications Cloud Native Core Policy	1.14.0	All
Application	Oracle	Communications Unified Inventory Management	7.3.4	All
Application	Oracle	Communications Unified Inventory Management	7.3.5	All

Application	Oracle	Communications Unified Inventory Management	7.4.0	All
Application	Oracle	Communications Unified Inventory Management	7.4.1	All
Application	Oracle	Communications Unified Inventory Management	7.4.2	All
Application	Oracle	Retail Xstore Point Of Service	16.0.6	All
Application	Oracle	Retail Xstore Point Of Service	17.0.4	All
Application	Oracle	Retail Xstore Point Of Service	18.0.3	All
Application	Oracle	Retail Xstore Point Of Service	19.0.2	All
Application	Oracle	Retail Xstore Point Of Service	20.0.1	All
Application	Oracle	Utilities Framework	4.2.0.2.0	All
Application	Oracle	Utilities Framework	4.2.0.3.0	All
Application	Oracle	Utilities Framework	4.3.0.1.0	All
Application	Oracle	Utilities Framework	4.3.0.6.0	All
Application	Oracle	Utilities Framework	4.4.0.0.0	All
Application	Oracle	Utilities Framework	4.4.0.2.0	All
Application	Oracle	Utilities Framework	4.4.0.3.0	All
Application	Oracle	Utilities Testing Accelerator	6.0.0.1.1	All
Application	Oracle	Webcenter Portal	12.2.1.3.0	All
Application	Oracle	Webcenter Portal	12.2.1.4.0	All
Application	Xstream Project	Xstream	All	All

References

Reference	Source	Link	Ta
XStream is vulnerable to an Arbitrary Code Execution attack · Advisory · x-stream/xstream · GitHub	CONFIRM	github.com	
XStream - CVE-2021-39149	MISC	x-stream.github.io	
[SECURITY] Fedora 34 Update: xstream-1.4.18-2.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
[SECURITY] [DLA 2769-1] libxstream-java security update	MLIST	lists.debian.org	
[SECURITY] Fedora 33 Update: xstream-1.4.18-2.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
Oracle Critical Patch Update Advisory - April 2022	MISC	www.oracle.com	
August 2021 XStream Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
Oracle Critical Patch Update Advisory - January 2022	MISC	www.oracle.com	
Debian -- Security Information -- DSA-5004-1 libxstream-java	DEBIAN	www.debian.org	
[SECURITY] Fedora 34 Update: xstream-1.4.18-2.fc34 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] Fedora 35 Update: xstream-1.4.18-2.fc35 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] Fedora 33 Update: xstream-1.4.18-2.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
[SECURITY] Fedora 35 Update: xstream-1.4.18-2.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	

Oracle Critical Patch Update Advisory - July 2022	N/A	www.oracle.com	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159437 Oracle Enterprise Linux Security Update for xstream (ELSA-2021-3956)
178813 Debian Security Update for libxstream-java (DLA 2769-1)
178889 Debian Security Update for libxstream-java (DSA 5004-1)
178890 Debian Security Update for libxstream-java (DSA 5004-1)
183243 Debian Security Update for libxstream-java (CVE-2021-39149)
199237 Ubuntu Security Notification for XStream Vulnerabilities (USN-5946-1)
239729 Red Hat Update for xstream (RHSA-2021:3956)
281980 Fedora Security Update for xstream (FEDORA-2021-d894ca87dc)
281981 Fedora Security Update for xstream (FEDORA-2021-fbad11014a)
353077 Amazon Linux Security Advisory for xstream : ALAS2-2021-1729
375827 XStream Arbitrary Code Execution And Multiple vulnerabilities
376998 Alibaba Cloud Linux Security Update for xstream (ALINUX2-SA-2021:0065)
751258 OpenSUSE Security Update for xstream (openSUSE-SU-2021:3476-1)
751298 OpenSUSE Security Update for xstream (openSUSE-SU-2021:1401-1)
980145 Java (maven) Security Update for com.thoughtworks.xstream:xstream (GHSA-3ccq-5vw3-2p6x)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report