

Software Vulnerability Research Release Notes

September 2023 - Update 2

Introduction	1
New Features and Enhancements	2
Vulnerability View Enhancements.....	2
System Requirements	3
Legal Information	4

Introduction

Software Vulnerability Research provides access to verified intelligence from Secunia Research, covering all applications and systems across all platforms. Prioritization is driven by threat intelligence, workflows, tickets and alerts, and describes the steps to mitigate the risk of costly breaches. You stay in control and hackers stay out. For more information, see <https://www.flexera.com/products/operations/software-vulnerability-research.html>

New Features and Enhancements

This Software Vulnerability Research update includes the following:

- [Vulnerability View Enhancements](#)

Vulnerability View Enhancements

In the **Research** menu > **Vulnerability Database** tab > **Vulnerabilities** page > **CVE Reference** popup, the following enhancements are added.

- **Affected watch lists**— Displays affected watch list details.
- **Related ticket**— By clicking on the related tickets, it navigates to the associated ticket.
- **NVD CVSS Column**— NVD CVSS link has been enabled. By clicking on the **CVSS** link, a popup appears with the detailed information related to the CVSS details.
- **Vulnerability Column**— By clicking CVE Reference link navigates to the cve.mitre.org website for cybersecurity vulnerabilities information for the specific CVE.

CVE-2023-43498

Vulnerability	NVD CVSS*	Threat Score	Threat Reason
CVE-2023-43498	CVSS v3: 8.1 CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C/I:L/A:N	15	Recently Linked to Penetration Testing Tools

Description*
In Jenkins 2.423 and earlier, LTS 2.414.1 and earlier, processing file uploads using MultipartFormDataParser creates temporary files in the default system temporary directory with the default permissions for newly created files, potentially allowing attackers with access to the Jenkins controller file system to read and write the files before they are used.

Threat Intel Module
The CVE threat score of 15 was based on the following triggers:
Recently Linked to Penetration Testing Tools

The threat score was last updated on 2023-09-21.

References*
Other Reference: <http://www.openwall.com/lists/oss-security/2023/09/20/5>
Other Reference: <https://www.jenkins.io/security/advisory/2023-09-20/#SECURITY-3073>

Advisories

Advisory	Release date	Modified date	Title	Criticality	Zero Day	Solution status	Where	CVSS Score	Threat Score	Type
SA119411	2023-09-21	2023-09-21	Jenkins Multiple Vulnerabilities		No	Vendor Patched	From remote	5.4 v3	15	Secunia Advisory

Affected watch lists

Watch List	CVSS Overall Score & Vector
	CVSS2: Overall: 0 (None)
	CVSS3: Overall: 4.7 CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C/I:L/A:N/E:U/R:L/O/R:C
	CVSS2: Overall: 0 (None)
	CVSS3: Overall: 4.7 CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C/I:L/A:N/E:U/R:L/O/R:C
	CVSS2: Overall: 0 (None)
	CVSS3: Overall: 4.7 CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C/I:L/A:N/E:U/R:L/O/R:C

Related tickets
[71790](#) | [71791](#) | [71792](#) | [71793](#) |

NOTE:
* The information is written and maintained by [CVE MITRE](#).
The data on this page reflects neither the opinions of Secunia or the results of our research.

System Requirements

Software Vulnerability Research's user interface will resize and adapt when being used on different devices. You can access the system from anywhere using any device, such as a smart phone or tablet, running Microsoft Edge, Chrome, Opera, Firefox, Safari and mobile browsers with an Internet connection capable of connecting to <https://app.flexerasoftware.com>.

Legal Information

Copyright Notice

Copyright © 2023 Flexera

This publication contains proprietary and confidential information and creative works owned by Flexera and its licensors, if any. Any use, copying, publication, distribution, display, modification, or transmission of such publication in whole or in part in any form or by any means without the prior express written permission of Flexera is strictly prohibited. Except where expressly provided by Flexera in writing, possession of this publication shall not be construed to confer any license or rights under any Flexera intellectual property rights, whether by estoppel, implication, or otherwise.

All copies of the technology and related information, if allowed by Flexera, must display this notice of copyright and ownership in full.

Intellectual Property

For a list of trademarks and patents that are owned by Flexera, see <https://www.flexera.com/legal/intellectual-property.html>. All other brand and product names mentioned in Flexera products, product documentation, and marketing materials are the trademarks and registered trademarks of their respective owners.

Restricted Rights Legend

The Software is commercial computer software. If the user or licensee of the Software is an agency, department, or other entity of the United States Government, the use, duplication, reproduction, release, modification, disclosure, or transfer of the Software, or any related documentation of any kind, including technical data and manuals, is restricted by a license agreement or by the terms of this Agreement in accordance with Federal Acquisition Regulation 12.212 for civilian purposes and Defense Federal Acquisition Regulation Supplement 227.7202 for military purposes. The Software was developed fully at private expense. All other use is prohibited.