



CVE-2023-40548

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-40548
State	RESERVED
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-01-29 15:15:00 UTC
Updated	2024-03-26 16:15:00 UTC
Description	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	39	All	All	All
Application	Redhat	Shim	All	All	All	All
Application	Redhat	Shim	15.8	rc1	All	All

References

Reference

[cve-details](#)

[2241782 – \(CVE-2023-40548\) CVE-2023-40548 shim: Interger overflow leads to heap buffer overflow in verify_sbata_section on 32-bits system](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[379359](#) Shim package Multiple Vulnerabilities

[673479](#) EulerOS Security Update for shim (EulerOS-SA-2024-1249)

[673479](#) EulerOS Security Update for shim (EulerOS-SA-2024-1249)

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)