



# CVE-2021-3695

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2021-3695
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-07-06 16:15:00 UTC
<b>Updated</b>	2023-09-13 16:15:00 UTC
<b>Description</b>	A crafted 16-bit grayscale PNG image may lead to a out-of-bounds write in the heap area. An attacker may take advantage

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	36	All
Application	<a href="#">Gnu</a>	<a href="#">Grub</a>	All	All
Application	<a href="#">Gnu</a>	<a href="#">Grub2</a>	All	All
Application	<a href="#">Netapp</a>	<a href="#">Ontap Select Deploy Administration Utility</a>	-	All
Application	<a href="#">Redhat</a>	<a href="#">Codeready Linux Builder</a>	-	All
Application	<a href="#">Redhat</a>	<a href="#">Developer Tools</a>	1.0	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	9.0	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.1	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.4	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	9.0	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	8.2	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	8.4	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	8.6	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	9.0	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	8.2	All

Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	8.4	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	8.6	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	9.0	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Power Little Endian</a>	8.0	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Power Little Endian</a>	9.0	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Power Little Endian Eus</a>	8.2	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Power Little Endian Eus</a>	8.4	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Power Little Endian Eus</a>	8.6	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Power Little Endian Eus</a>	9.0	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	8.2	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	8.4	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	8.6	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server For Power Little Endian Update Services For Sap Solutions</a>	8.1	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server For Power Little Endian Update Services For Sap Solutions</a>	8.2	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server For Power Little Endian Update Services For Sap Solutions</a>	8.4	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server For Power Little Endian Update Services For Sap Solutions</a>	8.6	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server For Power Little Endian Update Services For Sap Solutions</a>	9.0	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	8.2	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	8.4	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	8.6	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift</a>	3.0	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform</a>	4.10	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform</a>	4.6	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform</a>	4.9	All



## References

Reference	Source	L
July 2022 Grub Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	s
1991685 – (CVE-2021-3695) CVE-2021-3695 grub2: Crafted PNG grayscale images may lead to out-of-bounds write in heap	MISC	t
GRUB: Multiple Vulnerabilities (GLSA 202209-12) — Gentoo security	GENTOO	s
CVE Program record	CVE.ORG	v
NVD vulnerability detail	NVD	r



No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[159883](#) Oracle Enterprise Linux Security Update for grub2 (ELSA-2022-9471)

[159884](#) Oracle Enterprise Linux Security Update for grub2 (ELSA-2022-9469)

[159943](#) Oracle Enterprise Linux Security Update for grub2 (ELSA-2022-5099)

[159967](#) Oracle Enterprise Linux Security Update for grub2, mokutil, shim, and shim-unsigned-x64 (ELSA-2022-5095)

[159985](#) Oracle Enterprise Linux Security Update for grub2 (ELSA-2022-9596)

[159986](#) Oracle Enterprise Linux Security Update for grub2 (ELSA-2022-9595)

[161027](#) Oracle Enterprise Linux Security Update for grub2 (ELSA-2023-12952)

[181022](#) Debian Security Update for grub2 (CVE-2021-3695)

[240473](#) Red Hat Update for grub2, mokutil, shim, and shim-unsigned-x64 (RHSA-2022:5100)

[240474](#) Red Hat Update for grub2, mokutil, shim, and shim-unsigned-x64 (RHSA-2022:5099)

[240476](#) Red Hat Update for grub2, mokutil, shim, and shim-unsigned-x64 (RHSA-2022:5096)

[240477](#) Red Hat Update for grub2, mokutil, shim, and shim-unsigned-x64 (RHSA-2022:5095)

[282811](#) Fedora Security Update for grub2 (FEDORA-2022-27932fdd06)

[282866](#) Fedora Security Update for grub2 (FEDORA-2022-9b4f9af4ce)

[354332](#) Amazon Linux Security Advisory for grub2 : ALAS2022-2022-109

[354535](#) Amazon Linux Security Advisory for grub2 : ALAS-2022-109

[355137](#) Amazon Linux Security Advisory for grub2 : ALAS2023-2023-020

[355617](#) Amazon Linux Security Advisory for grub2 : ALAS2-2023-2146

[377130](#) Alibaba Cloud Linux Security Update for grub2, mokutil, shim, and shim-unsigned-x64 (ALINUX3-SA-2022:0134)

[377622](#) Alibaba Cloud Linux Security Update for grub2, mokutil, shim, and shim-unsigned-x64 (ALINUX3-SA-2022:0164)

[672021](#) EulerOS Security Update for grub2 (EulerOS-SA-2022-2242)

[672026](#) EulerOS Security Update for grub2 (EulerOS-SA-2022-2221)

[672031](#) EulerOS Security Update for grub2 (EulerOS-SA-2022-2255)

[672032](#) EulerOS Security Update for grub2 (EulerOS-SA-2022-2268)

[672109](#) EulerOS Security Update for grub2 (EulerOS-SA-2022-2318)

[672131](#) EulerOS Security Update for grub2 (EulerOS-SA-2022-2289)

[672248](#) EulerOS Security Update for grub2 (EulerOS-SA-2022-2611)

[710619](#) Gentoo Linux GRUB Multiple Vulnerabilities (GLSA 202209-12)

752214	SUSE Enterprise Linux Security Update for grub2 (SUSE-SU-2022:2037-1)
752215	SUSE Enterprise Linux Security Update for grub2 (SUSE-SU-2022:2041-1)
752216	SUSE Enterprise Linux Security Update for grub2 (SUSE-SU-2022:2036-1)
752217	SUSE Enterprise Linux Security Update for grub2 (SUSE-SU-2022:2035-1)
752218	SUSE Enterprise Linux Security Update for grub2 (SUSE-SU-2022:2038-1)
752221	SUSE Enterprise Linux Security Update for grub2 (SUSE-SU-2022:2064-1)
752229	SUSE Enterprise Linux Security Update for grub2 (SUSE-SU-2022:2074-1)
907566	Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (31034-1)
940639	AlmaLinux Security Update for grub2, (ALSA-2022:5095)
940640	AlmaLinux Security Update for grub2, (ALSA-2022:5099)
960155	Rocky Linux Security Update for grub2, (RLSA-2022:5095)
960538	Rocky Linux Security Update for grub2, (RLSA-2022:5099)

© [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](#)**