



# CVE-2022-2601

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

## Summary

<b>CVE</b>	CVE-2022-2601
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-12-14 21:15:00 UTC
<b>Updated</b>	2023-11-25 12:15:00 UTC
<b>Description</b>	A buffer overflow was found in grub_font_construct_glyph(). A malicious crafted pf2 font can lead to an overflow when calcul

## Risk And Classification

**Problem Types:** CWE-122

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	37	All
Application	<a href="#">Gnu</a>	<a href="#">Grub2</a>	All	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 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 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>	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 Update Services For Sap Solutions</a>	8.1	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Update Services For Sap Solutions</a>	8.2	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Update Services For Sap Solutions</a>	9.0	All

## References

### Reference

2112975 – (CVE-2022-2601) CVE-2022-2601 grub2: Buffer overflow in grub\_font\_construct\_glyph() can lead to out-of-bound write and possib

GRUB: Multiple Vulnerabilities (GLSA 202311-14) — Gentoo security

[CVE Program record](#)

[NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[160386](#) Oracle Enterprise Linux Security Update for grub2 (ELSA-2023-12019)

[160437](#) Oracle Enterprise Linux Security Update for grub2 (ELSA-2023-0049)

[160730](#) Oracle Enterprise Linux Security Update for grub2 (ELSA-2023-0752)

[181216](#) Debian Security Update for grub2 (DSA 5280-1)

[181218](#) Debian Security Update for grub2 (DLA 3190-1)

[181312](#) Debian Security Update for grub2 (DLA 3190-2)

[184689](#) Debian Security Update for grub2 (CVE-2022-2601)

[241007](#) Red Hat Update for grub2 (RHSA-2022:8978)

[241037](#) Red Hat Update for grub2 (RHSA-2023:0047)

[241040](#) Red Hat Update for grub2 (RHSA-2023:0048)

[241042](#) Red Hat Update for grub2 (RHSA-2023:0049)

[241185](#) Red Hat Update for grub2 (RHSA-2023:0752)

[283350](#) Fedora Security Update for grub2 (FEDORA-2022-f86e203baf)

[283365](#) Fedora Security Update for grub2 (FEDORA-2022-7ce9378e90)

[283416](#) Fedora Security Update for grub2 (FEDORA-2022-dec4cdacd7)

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

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

[377900](#) Alibaba Cloud Linux Security Update for grub2 (ALINUX3-SA-2023:0003)

[672578](#) EulerOS Security Update for grub2 (EulerOS-SA-2023-1317)

[672656](#) EulerOS Security Update for grub2 (EulerOS-SA-2023-1386)

[672662](#) EulerOS Security Update for grub2 (EulerOS-SA-2023-1358)

[672671](#) EulerOS Security Update for grub2 (EulerOS-SA-2023-1407)

[672699](#) EulerOS Security Update for grub2 (EulerOS-SA-2023-1409)

<a href="#">672093</a> EulerOS Security Update for grub2 (EulerOS-SA-2023-1422)
<a href="#">672717</a> EulerOS Security Update for grub2 (EulerOS-SA-2023-1443)
<a href="#">672766</a> EulerOS Security Update for grub2 (EulerOS-SA-2023-1468)
<a href="#">710796</a> Gentoo Linux GRUB Multiple Vulnerabilities (GLSA 202311-14)
<a href="#">752845</a> SUSE Enterprise Linux Security Update for grub2 (SUSE-SU-2022:4219-1)
<a href="#">752900</a> SUSE Enterprise Linux Security Update for grub2 (SUSE-SU-2022:4218-1)
<a href="#">752909</a> SUSE Enterprise Linux Security Update for grub2 (SUSE-SU-2022:4141-1)
<a href="#">752923</a> SUSE Enterprise Linux Security Update for grub2 (SUSE-SU-2022:4140-1)
<a href="#">752932</a> SUSE Enterprise Linux Security Update for grub2 (SUSE-SU-2022:4142-1)
<a href="#">752964</a> SUSE Enterprise Linux Security Update for grub2 (SUSE-SU-2022:4302-1)
<a href="#">904689</a> Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (11629)
<a href="#">904696</a> Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (11604)
<a href="#">905183</a> Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (11629-1)
<a href="#">905244</a> Common Base Linux Mariner (CBL-Mariner) Security Update for grub2 (11604-1)
<a href="#">940866</a> AlmaLinux Security Update for grub2 (ALSA-2023:0049)
<a href="#">940924</a> AlmaLinux Security Update for grub2 (ALSA-2023:0752)
<a href="#">960514</a> Rocky Linux Security Update for grub2 (RLSA-2023:0049)
<a href="#">960577</a> Rocky Linux Security Update for grub2 (RLSA-2023:0752)

© [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](#)**