



CVE-2022-2553

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

Summary

CVE	CVE-2022-2553
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-07-28 15:15:00 UTC
Updated	2023-11-07 03:46:00 UTC
Description	The authfile directive in the booth config file is ignored, preventing use of authentication in communications from node to no

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Clusterlabs	Booth	All	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 35 Update: booth-1.0-251.4.bfb2f92.git.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 36 Update: booth-1.0-262.3.d0ac26c.git.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 35 Update: booth-1.0-251.4.bfb2f92.git.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
Debian -- Security Information -- DSA-5194-1 booth	DEBIAN	www.debian.org
[SECURITY] Fedora 36 Update: booth-1.0-262.3.d0ac26c.git.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
cve-website	MISC	www.cve.org
Revert "Refactor: main: substitute is_auth_req macro" · ClusterLabs/booth@35bf0b7 · GitHub	MISC	github.com
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

180903	Debian Security Update for booth (DSA 5194-1)
183290	Debian Security Update for booth (CVE-2022-2553)
198900	Ubuntu Security Notification for Booth Vulnerability (USN-5556-1)
240642	Red Hat Update for booth (RHSA-2022:6250)
240657	Red Hat Update for booth (RHSA-2022:6439)
240685	Red Hat Update for booth (RHSA-2022:6580)
283188	Fedora Security Update for booth (FEDORA-2022-e0a87993b8)
283189	Fedora Security Update for booth (FEDORA-2022-6744980220)
354848	Amazon Linux Security Advisory for booth : ALAS2-2023-2009
753131	SUSE Enterprise Linux Security Update for booth (SUSE-SU-2022:2609-1)
753161	SUSE Enterprise Linux Security Update for booth (SUSE-SU-2022:2606-1)
753183	SUSE Enterprise Linux Security Update for booth (SUSE-SU-2022:2608-1)
753391	SUSE Enterprise Linux Security Update for booth (SUSE-SU-2022:2607-1)
907276	Common Base Linux Mariner (CBL-Mariner) Security Update for booth (25645-1)
940662	AlmaLinux Security Update for booth (ALSA-2022:6439)
940685	AlmaLinux Security Update for booth (ALSA-2022:6580)
960286	Rocky Linux Security Update for booth (RLSA-2022:6439)

© [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](#)