



CVE-2021-44273

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2021-44273
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-23 12:15:00 UTC
Updated	2023-09-13 00:15:00 UTC
Description	e2guardian v5.4.x <= v5.4.3r is affected by missing SSL certificate validation in the SSL MITM engine. In standalone mode

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	E2bn	E2guardian	All	All	All	All

References

Reference	Source	Link	Tags
[SECURITY] [DLA 3564-1] e2guardian security update	MLIST	lists.debian.org	
Fix bug #707 cert hostnames not being checked · e2guardian/e2guardian@eae46a7 · GitHub	MISC	github.com	
oss-security - CVE-2021-44273: e2guardian did not validate TLS hostnames	MLIST	www.openwall.com	
v5.4: Missing SSL hostname check · Issue #707 · e2guardian/e2guardian · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[179424](#) Debian Security Update for e2guardian (CVE-2021-44273)

[502559](#) Alpine Linux Security Update for e2guardian

[504730](#) Alpine Linux Security Update for e2guardian

© [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](#)