



CVE-2020-11000

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

Summary

CVE	CVE-2020-11000
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-08 17:15:00 UTC
Updated	2021-10-26 20:02:00 UTC
Description	GreenBrowser before version 1.2 has a vulnerability where apps that rely on URL Parsing to verify that a given URL is point

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Greenbrowser Project	Greenbrowser	All	All	All	All
Application	Greenbrowser Project	Greenbrowser	All	All	All	All

References

Reference	Source	Link	Tags
Improper URL validation · Advisory · luchua-bc/GreenBrowser · GitHub	CONFIRM	github.com	Third Party Advisory
Address the issue related to URL validation · luchua-bc/GreenBrowser@5e257e0 · GitHub	MISC	github.com	Patch, Third Party A
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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