



CVE-2020-15688

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

Summary

CVE	CVE-2020-15688
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-07-23 13:15:00 UTC
Updated	2023-01-31 17:25:00 UTC
Description	The HTTP Digest Authentication in the GoAhead web server before 5.1.2 does not completely protect against replay attack

Risk And Classification

Problem Types: CWE-294

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Embedthis	Goahead	All	All	All	All
Application	Embedthis	Goahead	All	All	All	All

References

Reference	Source	Link
Digest Nonce Handling over HTTP · Issue #3 · embedthis/goahead-gpl · GitHub	MISC	github.com
EmbedThis GoAhead Web Server 5.1.1 Digest Authentication Capture Replay Nonce Reuse ≈ Packet Storm	MISC	packetstormsecu
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)