CVE-2020-24708

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2020-24708
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-10-28 20:15:00 UTC
Updated	2020-10-29 20:51:00 UTC
Description	Cross Site Scripting (XSS) vulnerability in Gophish before 0.11.0 via the Host field on the send profile form.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Getgophish	Gophish	All	All	All	All
Application	Getgophish	Gophish	All	All	All	All

References

Reference	Source	Link	Tags
usd-2020-0048 | usd Herolab	MISC	herolab.usd.de	Exploit,
Added escaping for error message in sending profile hostname · gophish/gophish@90fed5a · GitHub	MISC	github.com	Patch,
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

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

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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