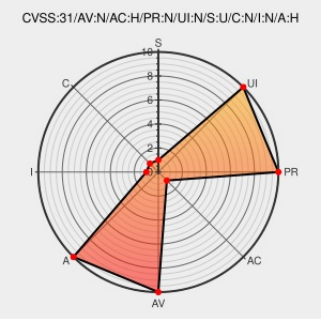
CVE-2022-29242

Published on: Not Yet Published

Last Modified on: 06/07/2022 04:54:00 PM UTC

CVE-2022-29242 - advisory for GHSA-2rmw-8wpg-vgw5

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Gost Engine from Gost Engine Project contain the following vulnerability:

GOST engine is a reference implementation of the Russian GOST crypto algorithms for OpenSSL. TLS clients using GOST engine when ciphersuite `TLS_GOSTR341112_256_WITH_KUZNYECHIK_CTR_OMAC` is agreed and the server uses 512 bit GOST secret keys are vulnerable to buffer overflow. GOST engine version 3.0.1 contains a patch for this issue. Disabling ciphersuite `TLS_GOSTR341112_256_WITH_KUZNYECHIK_CTR_OMAC` is a possible workaround.

CVE-2022-29242 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **gost-engine** - **engine** version **< 3.0.1**

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

CVE References

Description	Tags	Link
Fix buffer overrun in creating key transport blob according to RFC 91… · gost-engine/engine@c6655a0 · GitHub	github.com text/html	MISC github.com/gost-engine/engine/commit/c6655a0b620a3e31f085cc906f8073fe81b2fad3
Fix buffer overrun in creating key transport blob according to RFC 91… · gost-engine/engine@7df7661 · GitHub	github.com text/html	MISC github.com/gost-engine/engine/commit/7df766124f87768b43b9e8947c5a01e17545772c
On unpacking key blob output buffer size should be fixed · gost-engine/engine@b2b4d62 · GitHub	github.com text/html	MISC github.com/gost-engine/engine/commit/b2b4d629f100eaee9f5942a106b1ccefe85b8808
Release CVE-2022-29242 fix · gost-engine/engine · GitHub	github.com text/html	MISC github.com/gost-engine/engine/releases/tag/v3.0.1
Buffer overrun on creating key transport blob · Advisory · gost-engine/engine · GitHub	github.com text/html	CONFIRM github.com/gost-engine/engine/security/advisories/GHSA-2rmw-8wpg-vgw5

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gost Engine Project	Gost Engine	All	All	All	All

cpe:2.3:a:gost_engine_project:gost_engine:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-29242 : GOST engine is a reference implementation of the Russian GOST crypto algorithms for OpenSSL. TLS c… twitter.com/i/web/status/1…	2022-05-24 14:56:36
@LinInfoSec	Openssl - CVE-2022-29242: github.com/gost-engine/en…	2022-05-24 17:00:35
/r/netcve	CVE-2022-29242	2022-05-24 15:38:19

← Previous ID

Next ID→

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.

CVE.report and Source URL Uptime Status status.cve.report