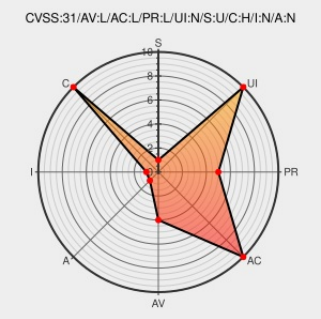
CVE-2023-42811

Published on: Not Yet Published

Last Modified on: 10/03/2023 04:15:00 AM UTC

CVE-2023-42811 - advisory for GHSA-423w-p2w9-r7vq

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



Certain versions of Aes-gcm from Aes-gcm Project contain the following vulnerability:

aes-gcm is a pure Rust implementation of the AES-GCM. Starting in version 0.10.0 and prior to version 0.10.3, in the AES GCM implementation of decrypt_in_place_detached, the decrypted ciphertext (i.e. the correct plaintext) is exposed even if tag verification fails. If a program using the `aes-gcm` crate's `decrypt_in_place*` APIs accesses the buffer after decryption failure, it will contain a decryption of an unauthenticated input. Depending on the specific nature of the program this may enable Chosen Ciphertext Attacks (CCAs) which can cause a catastrophic breakage of the cipher including full plaintext recovery. Version 0.10.3 contains a fix for this issue.

CVE-2023-42811 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **RustCrypto** - **AEADs** version **= >= 0.10.0, < 0.10.3**

CVSS3 Score: 5.5 - MEDIUM

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

CVE References

Description	Tags	Link
AEADs/aes-gcm: Plaintext exposed in decrypt_in_place_detached even on tag verification failure · Advisory ·	github.com text/html	MISC github.com/RustCrypto/AEADs/security/advisories/GHSA-423w-p2w9-r7vq

RustCrypto/AEADs · GitHub		
[SECURITY] Fedora 37 Update: rust-aes-gcm-0.10.3-1.fc37 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	MISC lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/U67ZSMNX5V3WTBYPUYF45PSFG4SF5S
[SECURITY] Fedora 38 Update: rust-aes-gcm-0.10.3-1.fc38 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	MISC lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/ROBB6TBDAGEQ2WIINR34F3DPSN3FND
lib.rs - source	docs.rs text/html	MISC docs.rs/aes-gcm/latest/src/aes_gcm/lib.rs.html#309
[SECURITY] Fedora 39 Update: rust-aes-gcm-0.10.3-1.fc39 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	MISC lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/RYQCICN6BVC6I75O3F6W4VK4J3MOYD

Related QID Numbers

284564 Fedora Security Update for firecracker (FEDORA-2023-bc40c7995e)

284566 Fedora Security Update for firecracker (FEDORA-2023-98f44d1c4c)

755080 SUSE Enterprise Linux Security Update for rage-encryption (SUSE-SU-2023:4060-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Aes-gcm Project	Aes-gcm	All	All	All	All

cpe:2.3:a:aes-gcm_project:aes-gcm:*:*:*:*:*:rust:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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