



CVE-2020-15237

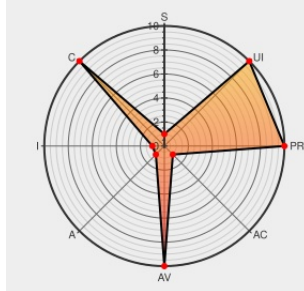
Published on: 10/05/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:40 PM UTC

CVE-2020-15237 - advisory for GHSA-5jjv-x4fq-qjwp

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N



Certain versions of [Shrine](#) from [Shrinerb](#) contain the following vulnerability:

In Shrine before version 3.3.0, when using the ``derivation_endpoint`` plugin, it's possible for the attacker to use a timing attack to guess the signature of the derivation URL. The problem has been fixed by comparing sent and calculated signature in constant time, using ``Rack::Utils.secure_compare``. Users using the ``derivation_endpoint``

plugin are urged to upgrade to Shrine 3.3.0 or greater. A possible workaround is provided in the linked advisory.

CVE-2020-15237 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: shrinerb - shrine version < 3.3.0

CVSS3 Score: **5.9 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description

Securely compare signature in derivation_endpoint · shrinerb/shrine@1b27090 · GitHub

Tags

Patch

Third Party Advisory

github.com

text/html

Link

MISC
github.com/shrinerb/shrine/commit/1b27090ce31543bf39f186c20ea47c8250fca2f0

Description

Possible timing attack in derivation_endpoint · Advisory · shrinerb/shrine · GitHub

Tags

Third Party Advisory

github.com

text/html

Link

CONFIRM
github.com/shrinerb/shrine/security/advisories/GHSA-5jjv-x4fq-qjwp

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Shrinerb	Shrine	All	All	All	All
Application	Shrinerb	Shrine	All	All	All	All

cpe:2.3:a:shrinerb:shrine:*:*:*:*:ruby:*:*:

cpe:2.3:a:shrinerb:shrine:*:*:*:*:ruby:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →