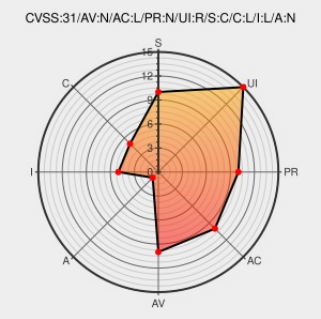
CVE-2018-3769

Published on: 07/05/2018 12:00:00 AM UTC

Last Modified on: 02/28/2023 05:54:00 PM UTC

CVE-2018-3769

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



Certain versions of Grape from Ruby-grape contain the following vulnerability:

ruby-grape ruby gem suffers from a cross-site scripting (XSS) vulnerability via "format" parameter.

CVE-2018-3769 has been assigned by support@hackerone.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Ruby Grape** - **ruby-grape ruby gem** version **>= 1.0.3**

CVSS3 Score: 6.1 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
When returning an HTML error, make sure it's safe (#1763) · ruby-grape/grape@6876b71 · GitHub	Patch, Third Party Advisory, github.com	CONFIRM github.com/ruby-grape/grape/commit/6876b71efc7b03f7ce1be3f075eaa4e7e6de19af

	text/html	
When returning an HTML error, make sure it's safe by ctennis · Pull Request #1763 · ruby-grape/grape · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/ruby-grape/grape/pull/1763
Default formatter error can cause XSS rendering issue · Issue #1762 · ruby-grape/grape · GitHub	Exploit Third Party Advisory github.com text/html	CONFIRM github.com/ruby-grape/grape/issues/1762

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ruby-grape	Grape	-	All	All	All
Application	Ruby-grape	Grape	-	All	All	All
Application	Ruby-grape	Grape	All	All	All	All

cpe:2.3:a:ruby-grape:grape:-:*:*:*:*:*:*:*:

cpe:2.3:a:ruby-grape:grape:-:*:*:*:*:*:*:*:

cpe:2.3:a:ruby-grape:grape:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→