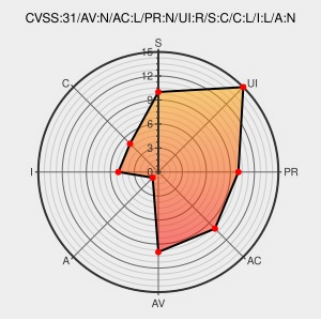
CVE-2019-25075

Published on: Not Yet Published

Last Modified on: 08/25/2022 06:22:00 PM UTC

CVE-2019-25075

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



Certain versions of Api Management from Gravitee contain the following vulnerability:

HTML injection combined with path traversal in the Email service in Gravitee API Management before 1.25.3 allows anonymous users to read arbitrary files via a /management/users/register request.

CVE-2019-25075 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

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

CVE References

Description	Tags	Link
GitHub - gravitee-io/gravitee-api-management: Gravitee.io - API Management - OpenSource API Gateway	github.com text/html	MISC github.com/gravitee-io/gravitee-api-management
Write-up for a Path Traversal on Gravitee.io | by Maxime Escourbiac | Medium	medium.com text/html	MISC medium.com/@maxime.escourbiac/write-up-of-path-traversal-on-gravitee-io-8835941be69f

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gravitee	Api Management	All	All	All	All

cpe:2.3:a:gravitee:api_management:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→