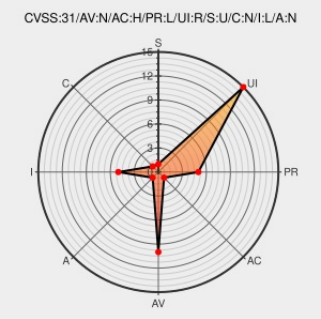
CVE-2018-25007

Published on: 04/23/2021 12:00:00 AM UTC

Last Modified on: 05/05/2021 06:26:00 PM UTC

CVE-2018-25007 - advisory for

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



Certain versions of Flow from Vaadin contain the following vulnerability:

Missing check in UIDL request handler in com.vaadin:flow-server versions 1.0.0 through 1.0.5 (Vaadin 10.0.0 through 10.0.7, and 11.0.0 through 11.0.2) allows attacker to update element property values via crafted synchronization message.

CVE-2018-25007 has been assigned by security@vaadin.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 4.3 - MEDIUM

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

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link
CVE-2018-25007: Unauthorized client-side property update in UIDL request handler in Vaadin 10 and 11	vaadin.com text/html	MISC vaadin.com/security/cve-2018-25007
Return back preventing disallowed property update by denis-anisimov · Pull Request	github.com	MISC

#4774 · vaadin/flow · GitHub text/html github.com/vaadin/flow/pull/4774

Related QID Numbers

982708 Java (maven) Security Update for com.vaadin:flow-server (GHSA-jmx8-355m-8vwh)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vaadin	Flow	All	All	All	All
Application	Vaadin	Vaadin	All	All	All	All

cpe:2.3:a:vaadin:flow:*:*:*:*:*:*:*:*:

cpe:2.3:a:vaadin:vaadin:*:*:*:*:*:*:*:*:

← Previous ID Next ID→