



CVE-2018-3783

Published on: 08/17/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:25 PM UTC

CVE-2018-3783

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

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

A privilege escalation detected in flintcms versions $\leq 1.1.9$ allows account takeover due to blind MongoDB injection in password reset.

CVE-2018-3783 has been assigned by [h1](#) support@hackerone.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [h1](#) <https://github.com/JasonEtco> - flintcms version 1.1.10

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
HackerOne	Exploit Patch Third Party Advisory	h1 MISC hackerone.com/reports/386807

Third Party Reference
hackerone.com
text/html

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.

Related QID Numbers

981012 Nodejs (npm) Security Update for flintcms (GHSA-jhq3-57xh-6643)

Exploit/POC from Github

Blind noSQL injection case study lab based on CVE-2018-3783

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Flintcms	Flintcms	All	All	All	All
cpe:2.3:a:flintcms:flintcms:*:*:*:*:node.js:*:*						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→