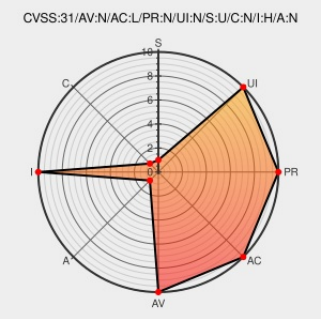
CVE-2017-18380

Published on: 07/30/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:55 PM UTC

CVE-2017-18380

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



Certain versions of Edx-platform from Edx contain the following vulnerability:

edx-platform before 2017-08-03 allows attackers to trigger password-reset e-mail messages in which the reset link has an attacker-controlled domain name.

CVE-2017-18380 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Google Groups	Mailing List, Third Party Advisory, groups.google.com, text/html	CONFIRM groups.google.com/forum/#!topic/openedx-announce/QTvijt48bAY

Mergeback PR from private to public. by edx-pipeline-bot · Pull Request #15773 · edx/edx-platform · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/edx/edx-platform/pull/15773

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Edx	Edx-platform	All	All	All	All
Application	Edx	Edx-platform	All	All	All	All

cpe:2.3:a:edx:edx-platform:*:*:*:*:*:*:*:*:

cpe:2.3:a:edx:edx-platform:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→