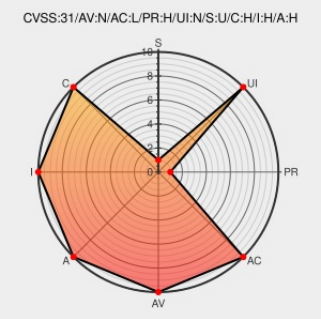
CVE-2020-7799

Published on: 01/28/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-7799

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



Certain versions of Fusionauth from Fusionauth contain the following vulnerability:

An issue was discovered in FusionAuth before 1.11.0. An authenticated user, allowed to edit e-mail templates (Home -> Settings -> Email Templates) or themes (Home -> Settings -> Themes), can execute commands on the underlying operating system by abusing freemarker.template.utility.Execute in the Apache FreeMarker engine that processes custom templates.

CVE-2020-7799 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.2 - HIGH

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

CVSS2 Score: 9 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
FusionAuth 1.10 Remote Command Execution ≈ Packet Storm	Third Party Advisory VDB Entry	MISC packetstormsecurity.com/files/156102/FusionAuth-

	packetstormsecurity.com text/html	1.10-Remote-Command-Execution.html
	Third Party Advisory lab.mediaservice.net text/plain	MISC lab.mediaservice.net/advisory/2020-03-fusionauth.txt
Bugtraq: CVE - CVE-2020-7799 - FusionAuth command execution via Apache Freemarker Template	Mailing List Third Party Advisory seclists.org text/html	BUGTRAQ 20200127 CVE - CVE-2020-7799 - FusionAuth command execution via Apache Freemarker Template
Release Notes - FusionAuth	Exploit Release Notes Vendor Advisory fusionauth.io text/html	MISC fusionauth.io/docs/v1/tech/release-notes

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fusionauth	Fusionauth	All	All	All	All
Application	Fusionauth	Fusionauth	All	All	All	All

cpe:2.3:a:fusionauth:fusionauth:*:*:*:*:*:*:*:*:

cpe:2.3:a:fusionauth:fusionauth:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→