



CVE-2020-7799

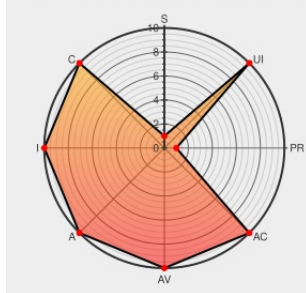
Published on: 01/28/2020 12:00:00 AM UTC

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

CVE-2020-7799

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

CVSS:31/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H



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 [M](#) [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

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report