

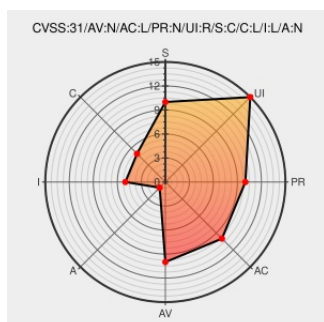


CVE-2020-26768

Published on: 01/07/2021 12:00:00 AM UTC

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

CVE-2020-26768

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

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

Formstone <=1.4.16 is vulnerable to a Reflected Cross-Site Scripting (XSS) vulnerability caused by improper validation of user supplied input in the upload-target.php and upload-chunked.php files. A remote attacker could exploit this vulnerability using a specially crafted URL to execute a script in a victim's Web browser within the security context of the hosting Web site once the URL is clicked or visited. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials, force malware execution, user redirection and others.

CVE-2020-26768 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
-------------	------	------

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Application	Formstone	Formstone	All	All	All	All
cpe:2.3:a:formstone:formstone:*.*.*.*.*.*.*.*.						

Next ID→