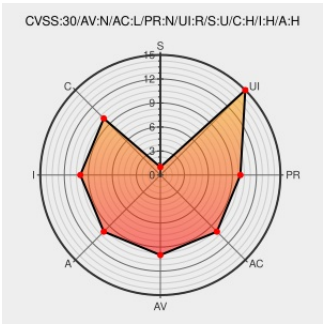
CVE-2019-1010094

Published on: 07/18/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:57 PM UTC

CVE-2019-1010094

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



Certain versions of Domainmod from Domainmod contain the following vulnerability:

domainmod v4.10.0 is affected by: Cross Site Request Forgery (CSRF). The impact is: There is a CSRF vulnerability that can change admin password. The component is: http://127.0.0.1/settings/password/ http://127.0.0.1/admin/users/add.php http://127.0.0.1/admin/users/edit.php?uid=2. The attack vector is: After the administrator logged in, open the html page.

CVE-2019-1010094 has been assigned by cve-assign@distributedweaknessfiling.org to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **DomainMOD** - **DomainMOD** version **v4.10.0**

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link

Description	Tags	Link
There are three CSRF vulnerability that can add the administrator account or change the read-only user to admin or change admin password · Issue #65 · domainmod/domainmod · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/domainmod/domainmod/issues/65

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Domainmod	Domainmod	4.10.0	All	All	All
Application	Domainmod	Domainmod	4.10.0	All	All	All

cpe:2.3:a:domainmod:domainmod:4.10.0:*:*:*:*:*:*:*

cpe:2.3:a:domainmod:domainmod:4.10.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→