

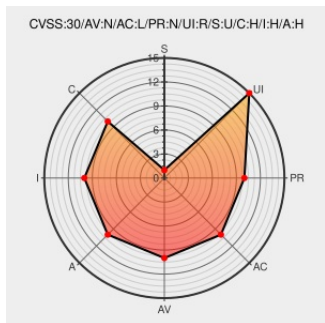


CVE-2017-6086

Published on: 06/27/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:50 PM UTC

CVE-2017-6086

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

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

Multiple cross-site request forgery (CSRF) vulnerabilities in the addAction and purgeAction functions in ViMbAdmin 3.0.15 allow remote attackers to hijack the authentication of logged administrators to (1) add an administrator user via a crafted POST request to <vimbadmin directory>/application/controllers/DomainController.php,

(2) remove an administrator user via a crafted GET request to <vimbadmin directory>/application/controllers/DomainController.php, (3) change an administrator password via a crafted POST request to <vimbadmin directory>/application/controllers/DomainController.php, (4) add a mailbox via a crafted POST request to <vimbadmin directory>/application/controllers/MailboxController.php, (5) delete a mailbox via a crafted POST request to <vimbadmin directory>/application/controllers/MailboxController.php, (6) archive a mailbox address via a crafted GET request to <vimbadmin directory>/application/controllers/ArchiveController.php, (7) add an alias address via a crafted POST request to <vimbadmin directory>/application/controllers/AliasController.php, or (8) remove an alias address via a crafted GET request to <vimbadmin directory>/application/controllers/AliasController.php.

CVE-2017-6086 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

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	Access	Authentication
--------	--------	----------------

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

CVE References

Description	Tags	Link
ViMAdmin 3.0.15 - Multiple Cross-Site Request Forgery Vulnerabilities - PHP webapps Exploit	www.exploit-db.com Proof of Concept text/html	 EXPLOIT-DB 41967
oss-security - [CVE-2017-6086] Multiple CSRF vulnerabilities in ViMAdmin version 3.0.15	Exploit Mailing List Third Party Advisory www.openwall.com text/html	 MLIST [oss-security] 20170503 [CVE-2017-6086] Multiple CSRF vulnerabilities in ViMAdmin version 3.0.15

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vimbadadmin	Vimbadadmin	3.0.15	All	All	All
Application	Vimbadadmin	Vimbadadmin	3.0.15	All	All	All
cpe:2.3:a:vimbadadmin:vimbadadmin:3.0.15:*****:.*						
cpe:2.3:a:vimbadadmin:vimbadadmin:3.0.15:*****:.*						

No vendor comments have been submitted for this CVE