CVE-2017-5930

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-5930
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-20 16:59:00 UTC
Updated	2020-02-26 16:59:00 UTC
Description	The AliasHandler component in PostfixAdmin before 3.0.2 allows remote authenticated domain admins to delete protected

Risk And Classification

Problem Types: CWE-862

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Leap	42.2	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Leap	42.2	All	All	All
Application	Postfixadmin Project	Postfixadmin	All	All	All	All
Application	Postfixadmin Project	Postfixadmin	All	All	All	All

References

Reference	Source	Link
Postfix Admin / [Postfixadmin-devel] Security hole in AliasHandler	MLIST	sourceforge.net
PostfixAdmin CVE-2017-5930 Session Management Security Bypass Vulnerability	BID	www.securityfocus.com
oss-security - Re: CVE request: PostfixAdmin allows to delete protected aliases	MLIST	www.openwall.com
openSUSE-SU-2017:0488-1: moderate: Security update for postfixadmin	SUSE	lists.opensuse.org
postfixadmin/CHANGELOG.TXT at postfixadmin-3.0.2 · postfixadmin/postfixadmin · GitHub	CONFIRM	github.com
oss-security - Re: CVE request: PostfixAdmin allows to delete protected aliases	MLIST	www.openwall.com
Fix security hole in AliasHandler by Janfred · Pull Request #23 · postfixadmin/postfixadmin · GitHub	CONFIRM	github.com
CVE Program record	CVE.ORG	www.cve.org

NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

501360 Alpine Linux Security Update for postfixadmin

Free CVE JSON API cve.report/api

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