CVE-2010-2053

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

Summary

CVE	CVE-2010-2053
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-06-07 17:13:00 UTC
Updated	2017-08-17 01:32:00 UTC
Description	emesenelib/ProfileManager.py in emesene before 1.6.2 allows local users to overwrite arbitrary files via a symlink attack on

Risk And Classification

Problem Types: CWE-59

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Emesene	Emesene	1.0	All	All	All
Application	Emesene	Emesene	1.0.1	All	All	All
Application	Emesene	Emesene	1.5	All	All	All
Application	Emesene	Emesene	1.5.1	All	All	All
Application	Emesene	Emesene	1.6	All	All	All
Application	Emesene	Emesene	1.0	All	All	All
Application	Emesene	Emesene	1.0.1	All	All	All
Application	Emesene	Emesene	1.5	All	All	All
Application	Emesene	Emesene	1.5.1	All	All	All
Application	Emesene	Emesene	1.6	All	All	All
Application	Emesene	Emesene	All	All	All	All

References

Reference	Source	Link	Tags
65018	OSVDB	osvdb.org	
'[oss-security] Fwd: emesene preditable temporary filename' - MARC	MLIST	marc.info	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com	

emesene	CONFIRM	www.emesene.org	
Fedora update for emesene - Advisories - Community	SECUNIA	secunia.com	
forum.emesene.org/index.php	CONFIRM	forum.emesene.org	Patch
emesene ProfileManager Insecure Temporary File - Secunia.com	SECUNIA	secunia.com	Vendor Advisory
[SECURITY] Fedora 13 Update: emesene-1.6.2-1.fc13	FEDORA	lists.fedoraproject.org	
emesene '/tmp/emsnpic' Insecure Temporary File Creation Vulnerability	BID	www.securityfocus.com	
[SECURITY] Fedora 11 Update: emesene-1.6.2-1.fc11	FEDORA	lists.fedoraproject.org	
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
[SECURITY] Fedora 12 Update: emesene-1.6.2-1.fc12	FEDORA	lists.fedoraproject.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.