CVE-2007-4138

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

Summary

CVE	CVE-2007-4138
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-09-14 01:17:00 UTC
Updated	2018-10-15 21:33:00 UTC
Description	The Winbind nss_info extension (nsswitch/idmap_ad.c) in idmap_ad.so in Samba 3.0.25 through 3.0.25c, when the "winbin

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Samba	Samba	3.0.25	All	All	All
Application	Samba	Samba	3.0.25a	All	All	All
Application	Samba	Samba	3.0.25b	All	All	All
Application	Samba	Samba	3.0.25c	All	All	All
Application	Samba	Samba	3.0.25	All	All	All
Application	Samba	Samba	3.0.25a	All	All	All
Application	Samba	Samba	3.0.25b	All	All	All
Application	Samba	Samba	3.0.25c	All	All	All

References

Reference	Source
SecurityReason - Winbind's rfc2307 & SFU nss_info plugin in Samba 3.0.25[a-c] assigns users a primary gid of 0 by default	SREASON
SecurityFocus	BUGTRAQ
[SECURITY] Fedora 7 Update: samba-3.0.26a-0.fc7	FEDORA
US-CERT Technical Cyber Security Alert TA07-352A -- Apple Updates for Multiple Vulnerabilities	CERT
IBM X-Force Exchange	XF
About Security Update 2007-009	CONFIRM

Repository / Oval Repository	OVAL
rhn.redhat.com | Red Hat Support	REDHAT
Samba Winbind SFU/RFC2307 GID Error Lets Local Users Gain Elevated Privileges - SecurityTracker	SECTRACK
Samba NSS_Info Plugin Local Privilege Escalation Vulnerability	BID
rhn.redhat.com | Red Hat Support	REDHAT
Samba "winbind nss info" Privilege Escalation Security Issue - Advisories - Secunia	SECUNIA
The Slackware Linux Project: Slackware Security Advisories	SLACKWARE
issues.rpath.com/browse/RPL-1705	CONFIRM
Webmail - OVH	VUPEN
Samba - Security Announcement Archive	CONFIRM
Fedora update for samba - Secunia.com	SECUNIA
Slackware update for samba - Advisories - Secunia	SECUNIA
rPath update for samba and samba-swat - Advisories - Secunia	SECUNIA
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2007-09-18	Mark J Cox	Not vulnerable. These issues did not affect the versions of Samba as shipped with Red Hat Ente

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