CVE-2008-1940

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

Summary

CVE	CVE-2008-1940
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-04-25 06:05:00 UTC
Updated	2017-08-08 01:30:00 UTC
Description	The RBAC functionality in grsecurity before 2.1.11-2.6.24.5 and 2.1.11-2.4.36.2 does not enforce user_transition_deny and

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Grsecurity	Grsecurity Kernel Patch	2.4.33	All	All	All
Application	Grsecurity	Grsecurity Kernel Patch	2.4.33.2	All	All	All
Application	Grsecurity	Grsecurity Kernel Patch	2.4.33.3	All	All	All
Application	Grsecurity	Grsecurity Kernel Patch	2.4.33.4	All	All	All
Application	Grsecurity	Grsecurity Kernel Patch	2.4.34	All	All	All
Application	Grsecurity	Grsecurity Kernel Patch	2.6.18	All	All	All
Application	Grsecurity	Grsecurity Kernel Patch	2.6.24.4	All	All	All
Application	Grsecurity	Grsecurity Kernel Patch	2.4.33	All	All	All
Application	Grsecurity	Grsecurity Kernel Patch	2.4.33.2	All	All	All
Application	Grsecurity	Grsecurity Kernel Patch	2.4.33.3	All	All	All
Application	Grsecurity	Grsecurity Kernel Patch	2.4.33.4	All	All	All
Application	Grsecurity	Grsecurity Kernel Patch	2.4.34	All	All	All
Application	Grsecurity	Grsecurity Kernel Patch	2.6.18	All	All	All
Application	Grsecurity	Grsecurity Kernel Patch	2.6.24.4	All	All	All

References

Reference	Source	Link	Ta

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com	
grsecurity	CONFIRM	www.grsecurity.org	
grsecurity RBAC User Transition Security Issue - Advisories - Secunia	SECUNIA	secunia.com	Pa
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
grsecurity Lets Local Users Bypass Role Based Access Control Rules - SecurityTracker	SECTRACK	www.securitytracker.com	
grsecurity Multiple RBAC Local Security Bypass Vulnerabilities	BID	www.securityfocus.com	Pa
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

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