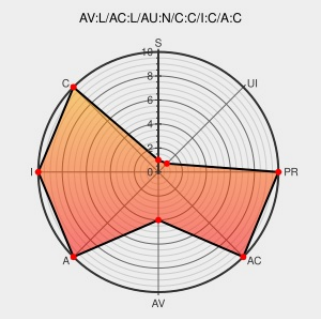
CVE-2005-3629

Published on: 12/31/2005 05:00:00 AM UTC

Last Modified on: 02/13/2023 02:10:42 AM UTC

CVE-2005-3629

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Enterprise Linux from Redhat contain the following vulnerability:

initscripts in Red Hat Enterprise Linux 4 does not properly handle certain environment variables when /sbin/service is executed, which allows local users with sudo permissions for /sbin/service to gain root privileges via unknown vectors.

CVE-2005-3629 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
SecurityTracker.com Archives - Red Hat initscripts Environment Variable Processing May Let Local Users Gain Elevated Privileges	Patch, Vendor Advisory, securitytracker.com, text/html	SECTRACK 1015732
Repository / Oval Repository	oval.cisecurity.org, text/html	OVAL oval:org.mitre.oval:def:11198
Secunia - Advisories - Red Hat update for initscripts	Patch, Vendor Advisory, web.archive.org, text/html	SECUNIA 19162
rhn.redhat.com | Red Hat Support	Patch, Vendor Advisory, www.redhat.com, text/html	REDHAT RHSA-2006:0016

No Description Provided	patches.sgi.com Inactive Link Not Archived	SGI 20060401-01-U
rhn.redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2006:0015
Red Hat Initscripts Local Privilege Escalation Vulnerability	cve.report (archive) text/html	BID 17038
SGI Advanced Linux Environment Multiple Updates - Advisories - Secunia	web.archive.org text/html	SECUNIA 19532
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF initscripts-service-gain-privileges(25374)

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Redhat	Enterprise Linux	3.0	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	workstation_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	workstation	All
Operating System	Redhat	Enterprise Linux	3.0	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	workstation_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	workstation	All

cpe:2.3:o:redhat:enterprise_linux:3.0:*:advanced_server:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:3.0:*:enterprise_server:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:3.0:*:workstation_server:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:4.0:*:advanced_server:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:4.0:*:enterprise_server:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:4.0:*:workstation:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:3.0:*:advanced_server:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:3.0:*:enterprise_server:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:3.0:*:workstation_server:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:4.0:*:advanced_server:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:4.0:*:enterprise_server:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:4.0:*:workstation:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→