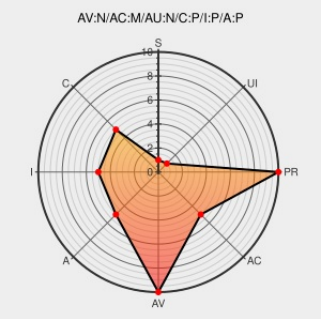
CVE-2009-0577

Published on: 02/20/2009 12:00:00 AM UTC

Last Modified on: 02/13/2023 02:19:00 AM UTC

CVE-2009-0577

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



Certain versions of Cups from Apple contain the following vulnerability:

Integer overflow in the WriteProlog function in texttops in CUPS 1.1.17 on Red Hat Enterprise Linux (RHEL) 3 allows remote attackers to execute arbitrary code via a crafted PostScript file that triggers a heap-based buffer overflow. NOTE: this issue exists because of an incorrect fix for CVE-2008-3640.

CVE-2009-0577 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Support	Patch, Vendor Advisory, www.redhat.com, text/html	REDHAT RHSA-2009:0308
Red Hat update for cups - Secunia Advisories - Vulnerability Information - Secunia.com	Permissions Required, Third Party Advisory, web.archive.org, text/html	SECUNIA 33995
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF cups-texttops-writeprolog-bo(48977)
Repository / Oval Repository	oval.cisecurity.org, text/html	OVAL oval:org.mitre.oval:def:9968
486052 – (CVE-2009-0577) CVE-2009-0577 cups-CVE-	Issue Tracking	CONFIRM

2008-3640.patch has been corrupted.	bugzilla.redhat.com text/html	bugzilla.redhat.com/show_bug.cgi?id=486052
ASA-2009-064 (RHSA-2009-0308)	Third Party Advisory support.avaya.com text/html	CONFIRM support.avaya.com/elmodocs2/security/ASA-2009-064.htm

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apple	Cups	1.1.17	All	All	All
Application	Apple	Cups	1.1.17	All	All	All
Operating System	Redhat	Enterprise Linux	3	All	All	All
Operating System	Redhat	Enterprise Linux	3	All	All	All

cpe:2.3:a:apple:cups:1.1.17:*:*:*:*:*:*:*:

cpe:2.3:a:apple:cups:1.1.17:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:3:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:3:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→