CVE-2010-2941

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

Summary

CVE	CVE-2010-2941
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-11-05 17:00:01 UTC
Updated	2026-04-29 01:13:23 UTC
Description	ipp.c in cupsd in CUPS 1.4.4 and earlier does not properly allocate memory for attribute values with invalid string data types

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Problem Types: CWE-416 | n/a

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	9.3		AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:M/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apple	Cups	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Apple	Mac Os X Server	All	All	All	All
Operating System	Apple	Mac Os X Server	All	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.10	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.10	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Fedoraproject	Fedora	12	All	All	All
Operating System	Fedoraproject	Fedora	13	All	All	All
Operating System	Fedoraproject	Fedora	14	All	All	All
Operating System	Opensuse	Opensuse	11.1	All	All	All
Operating System	Opensuse	Opensuse	11.2	All	All	All
Operating System	Opensuse	Opensuse	11.3	All	All	All

Operating System	Redhat	Enterprise Linux	5.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All
Operating System	Suse	Linux Enterprise	10.0	sp3	All	All
Operating System	Suse	Linux Enterprise	11.0	-	All	All
Operating System	Suse	Linux Enterprise	11.0	sp1	All	All
Operating System	Suse	Linux Enterprise Server	9	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
[SECURITY] Fedora 14 Update: cups-1.4.4-11.fc14	af854a3a-2127-422b-91ae
rhn.redhat.com | Red Hat Support	af854a3a-2127-422b-91ae
[SECURITY] Fedora 13 Update: cups-1.4.4-11.fc13	af854a3a-2127-422b-91ae
CUPS Server 'cups/ipp.c' Remote Memory Corruption Vulnerability	af854a3a-2127-422b-91ae
About the security content of Mac OS X v10.6.5 and Security Update 2010-007	af854a3a-2127-422b-91ae
APPLE-SA-2010-11-10-1 Mac OS X v10.6.5 and Security Update 2010-007	af854a3a-2127-422b-91ae
The Slackware Linux Project: Slackware Security Advisories	af854a3a-2127-422b-91ae
Support	af854a3a-2127-422b-91ae
Debian update for cups - Secunia.com	af854a3a-2127-422b-91ae
Security	af854a3a-2127-422b-91ae
Support / Security / Advisories / / MDVSA-2010:232 | Mandriva	af854a3a-2127-422b-91ae
Debian -- Security Information -- DSA-2176-1 cups	af854a3a-2127-422b-91ae
USN-1012-1: CUPS vulnerability | Ubuntu	af854a3a-2127-422b-91ae
Gentoo Linux Documentation -- CUPS: Multiple vulnerabilities	af854a3a-2127-422b-91ae
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae
IBM X-Force Exchange	af854a3a-2127-422b-91ae
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae
[SECURITY] Fedora 12 Update: cups-1.4.4-11.fc12	af854a3a-2127-422b-91ae
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae
Support / Security / Advisories / / MDVSA-2010:233 | Mandriva	af854a3a-2127-422b-91ae

[security-announce] SUSE Security Summary Report: SUSE-SR:2010:023	af854a3a-2127-422b-91ae
SecurityTracker.com Archives - CUPS IPP Request Processing Bug Lets Remote Users Execute Arbitrary Code	af854a3a-2127-422b-91ae
www.osvdb.org/68951	af854a3a-2127-422b-91ae
Support / Security / Advisories / / MDVSA-2010:234 | Mandriva	af854a3a-2127-422b-91ae
Oracle Solaris Firefox Multiple Vulnerabilities - Advisories - Community	af854a3a-2127-422b-91ae
624438 – (CVE-2010-2941) CVE-2010-2941 cups: cupsd memory corruption vulnerability	af854a3a-2127-422b-91ae
Fedora update for cups - Secunia.com	af854a3a-2127-422b-91ae
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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