



CVE-2012-3272

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2012-3272
State	PUBLIC
Assigner	hp-security-alert@hp.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-12-06 11:45:00 UTC
Updated	2013-01-08 05:03:00 UTC
Description	Cross-site scripting (XSS) vulnerability on the HP Color LaserJet CM3530 with firmware before 53.190.9, Color LaserJet CM

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Hp	Color Laserjet Cm3530	All	All	All	All
Hardware	Hp	Color Laserjet Cm60xx	All	All	All	All
Hardware	Hp	Color Laserjet Cp3525	All	All	All	All
Hardware	Hp	Color Laserjet Cp4xxx	All	All	All	All
Hardware	Hp	Color Laserjet Cp6015	All	All	All	All
Hardware	Hp	Laserjet P3015	All	All	All	All
Hardware	Hp	Laserjet P4xxx	All	All	All	All

References

Reference	Source	Link
Official HP® Support	HP	h20566...
HP LaserJet and Color LaserJet Printer Input Validation Flaw Permits Cross-Site Scripting Attacks - SecurityTracker	SECTRACK	www.se...
CVE Program record	CVE.ORG	www.cve...
NVD vulnerability detail	NVD	nvd.nist...

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)