



# CVE-2019-10627

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2019-10627
<b>State</b>	PUBLIC
<b>Assigner</b>	product-security@qualcomm.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-11-21 15:15:00 UTC
<b>Updated</b>	2022-04-12 18:41:00 UTC
<b>Description</b>	Integer overflow to buffer overflow vulnerability in PostScript image handling code used by the PostScript- and PDF-compat

## Risk And Classification

**Problem Types:** [CWE-119](#) | [CWE-190](#) | [CWE-131](#)

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Hp</a>	<a href="#">2dr21d</a>	-	All	All	All
Operating System	<a href="#">Hp</a>	<a href="#">2dr21d Firmware</a>	All	All	All	All
Hardware	<a href="#">Hp</a>	<a href="#">D3q15a</a>	-	All	All	All
Operating System	<a href="#">Hp</a>	<a href="#">D3q15a Firmware</a>	All	All	All	All
Hardware	<a href="#">Hp</a>	<a href="#">D3q15b</a>	-	All	All	All
Operating System	<a href="#">Hp</a>	<a href="#">D3q15b Firmware</a>	All	All	All	All
Hardware	<a href="#">Hp</a>	<a href="#">D3q15d</a>	-	All	All	All
Operating System	<a href="#">Hp</a>	<a href="#">D3q15d Firmware</a>	All	All	All	All
Hardware	<a href="#">Hp</a>	<a href="#">D3q16a</a>	-	All	All	All
Operating System	<a href="#">Hp</a>	<a href="#">D3q16a Firmware</a>	All	All	All	All
Hardware	<a href="#">Hp</a>	<a href="#">D3q16d</a>	-	All	All	All
Operating System	<a href="#">Hp</a>	<a href="#">D3q16d Firmware</a>	All	All	All	All
Hardware	<a href="#">Hp</a>	<a href="#">D3q17a</a>	-	All	All	All
Operating System	<a href="#">Hp</a>	<a href="#">D3q17a Firmware</a>	All	All	All	All
Hardware	<a href="#">Hp</a>	<a href="#">D3q17d</a>	-	All	All	All
Operating System	<a href="#">Hp</a>	<a href="#">D3q17d Firmware</a>	All	All	All	All
Hardware	<a href="#">Hp</a>	<a href="#">D3q19a</a>	-	All	All	All

Operating System	Hp	D3q19a Firmware	All	All	All	All
Hardware	Hp	D3q19b	-	All	All	All
Operating System	Hp	D3q19b Firmware	All	All	All	All
Hardware	Hp	D3q19d	-	All	All	All
Operating System	Hp	D3q19d Firmware	All	All	All	All
Hardware	Hp	D3q20a	-	All	All	All
Operating System	Hp	D3q20a Firmware	All	All	All	All
Hardware	Hp	D3q20b	-	All	All	All
Operating System	Hp	D3q20b Firmware	All	All	All	All
Hardware	Hp	D3q20c	-	All	All	All
Operating System	Hp	D3q20c Firmware	All	All	All	All
Hardware	Hp	D3q20d	-	All	All	All
Operating System	Hp	D3q20d Firmware	All	All	All	All
Hardware	Hp	D3q21a	-	All	All	All
Operating System	Hp	D3q21a Firmware	All	All	All	All
Hardware	Hp	D3q21b	-	All	All	All
Operating System	Hp	D3q21b Firmware	All	All	All	All
Hardware	Hp	D3q21c	-	All	All	All
Operating System	Hp	D3q21c Firmware	All	All	All	All
Hardware	Hp	D3q21d	-	All	All	All
Operating System	Hp	D3q21d Firmware	All	All	All	All
Hardware	Hp	D9l63a	-	All	All	All
Operating System	Hp	D9l63a Firmware	All	All	All	All
Hardware	Hp	D9l64a	-	All	All	All
Operating System	Hp	D9l64a Firmware	All	All	All	All
Hardware	Hp	J3p65a	-	All	All	All
Operating System	Hp	J3p65a Firmware	All	All	All	All
Hardware	Hp	J3p68a	-	All	All	All
Operating System	Hp	J3p68a Firmware	All	All	All	All
Hardware	Hp	J6u51b	-	All	All	All
Operating System	Hp	J6u51b Firmware	All	All	All	All
Hardware	Hp	J6u55a	-	All	All	All
Operating System	Hp	J6u55a Firmware	All	All	All	All
Hardware	Hp	J6u55d	-	All	All	All
Operating System	Hp	J6u55d Firmware	All	All	All	All

Hardware	Hp	J6u57a	-	All	All	All
Operating System	Hp	J6u57a Firmware	All	All	All	All
Hardware	Hp	J6u57b	-	All	All	All
Operating System	Hp	J6u57b Firmware	All	All	All	All
Hardware	Hp	J9v78b	-	All	All	All
Operating System	Hp	J9v78b Firmware	All	All	All	All
Hardware	Hp	J9v80a	-	All	All	All
Operating System	Hp	J9v80a Firmware	All	All	All	All
Hardware	Hp	J9v80b	-	All	All	All
Operating System	Hp	J9v80b Firmware	All	All	All	All
Hardware	Hp	J9v82a	-	All	All	All
Operating System	Hp	J9v82a Firmware	All	All	All	All
Hardware	Hp	J9v82d	-	All	All	All
Operating System	Hp	J9v82d Firmware	All	All	All	All
Hardware	Hp	K9z74a	-	All	All	All
Operating System	Hp	K9z74a Firmware	All	All	All	All
Hardware	Hp	K9z74d	-	All	All	All
Operating System	Hp	K9z74d Firmware	All	All	All	All
Hardware	Hp	K9z76a	-	All	All	All
Operating System	Hp	K9z76a Firmware	All	All	All	All
Hardware	Hp	K9z76b	-	All	All	All
Operating System	Hp	K9z76b Firmware	All	All	All	All
Hardware	Hp	K9z76d	-	All	All	All
Operating System	Hp	K9z76d Firmware	All	All	All	All
Hardware	Hp	T0g70a	-	All	All	All
Operating System	Hp	T0g70a Firmware	All	All	All	All
Hardware	Hp	W2z52b	-	All	All	All
Operating System	Hp	W2z52b Firmware	All	All	All	All
Hardware	Hp	W2z53b	-	All	All	All
Operating System	Hp	W2z53b Firmware	All	All	All	All
Application	Qualcomm	Ips	All	All	All	All
Application	Qualcomm	Ips	All	All	All	All

## References

Reference	Source	Link
HPSPBI03630 rev. 2 - HP Inkjet Printers - Buffer Overflow and Local Disclosure of Information   HP® Customer Support	MISC	<a href="#">suppo</a>

October Security Bulletin 2019   Qualcomm	CONFIRM	<a href="#">www.c</a>
CVE Program record	CVE.ORG	<a href="#">www.c</a>
NVD vulnerability detail	NVD	<a href="#">nvd.ni</a>

---

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](#)