



CVE-2015-6585

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

Summary

CVE	CVE-2015-6585
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-07-25 18:29:00 UTC
Updated	2017-08-10 13:25:00 UTC
Description	hwpapp.dll in Hangul Word Processor allows remote attackers to execute arbitrary code via a crafted heap spray, and by le

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hancom	Hangul Word Processor	2014	All	All	All
Application	Hancom	Hangul Word Processor	2014	All	All	All

References

Reference	Source	Link
,	CONFIRM	www.hancom.com
Zero-Day HWP Exploit « Threat Research FireEye Inc	MISC	www.fireeye.com
www.fireeye.com/content/dam/fireeye-www/global/en/blog/threat-research/FireEy...	MISC	www.fireeye.com
Hancom Hangul Word Processor CVE-2015-6585 Type Confusion Remote Code Execution Vulnerability	BID	www.securityfocus.co
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)