



CVE-2007-2347

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

Summary

CVE	CVE-2007-2347
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-04-27 17:19:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	PHP remote file inclusion vulnerability in main/forum/komentar.php in OneClick CMS (aka Sisplet CMS) 05.10 and earlier a

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:P/I:P/A:P

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Oneclick Cms	Oneclick Cms	All	All	All	All

Application	Sisplet Cms	Sisplet Cms	All	All	All	All
Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		
References						
Reference			Source	Link		
osvdb.org/35618			af854a3a-2127-422b-91ae-364da2661108	osvdb.org		
Sisplet CMS Komentar.PHP Remote File Include Vulnerability			af854a3a-2127-422b-91ae-364da2661108	www.securityfocus.com		
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH			af854a3a-2127-422b-91ae-364da2661108	www.vupen.com		
Sisplet CMS 05.10 - 'site_path' Remote File Inclusion - PHP webapps Exploit			af854a3a-2127-422b-91ae-364da2661108	www.exploit-db.com		
IBM X-Force Exchange			af854a3a-2127-422b-91ae-364da2661108	exchange.xforce.com		
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 |

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