



CVE-2010-2330

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

Summary

CVE	CVE-2010-2330
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-06-18 20:30:00 UTC
Updated	2017-08-17 01:32:00 UTC
Description	Stack-based buffer overflow in iSharer File Sharing Wizard 1.5.0 allows remote attackers to cause a denial of service (crash)

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Upredsun	Isharer File Sharing Wizard	1.5.0	All	All	All
Application	Upredsun	Isharer File Sharing Wizard	1.5.0	All	All	All

References

Reference	Source
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VULN
File Sharing Wizard v1.5.0 Buffer Overflow PoC	EXPL
File Sharing Wizard 'Content-Length' Header Buffer Overflow Vulnerability	BID
IBM X-Force Exchange	XF
Advisory: File Sharing Wizard - Buffer overflow vulnerability with overwritten EAX CPU register [Update: 20.06.2010] www.s3cur1ty.de	MISC
65570	OSV
File Sharing Wizard Two Buffer Overflow Vulnerabilities - Advisories - Community	SEC
CVE Program record	CV
NVD vulnerability detail	NVD

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](#)