CVE-2006-4161

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

Summary

CVE	CVE-2006-4161
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-08-16 22:04:00 UTC
Updated	2018-10-17 21:33:00 UTC
Description	Directory traversal vulnerability in the avatar_gallery action in profile.php in XennoBB 2.1.0 and earlier allows remote attack

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xennobb	Xennobb	1.0	All	All	All
Application	Xennobb	Xennobb	1.0.1	All	All	All
Application	Xennobb	Xennobb	1.0.2	All	All	All
Application	Xennobb	Xennobb	1.0.3	All	All	All
Application	Xennobb	Xennobb	1.0.4	All	All	All
Application	Xennobb	Xennobb	1.0.5	All	All	All
Application	Xennobb	Xennobb	1.0	All	All	All
Application	Xennobb	Xennobb	1.0.1	All	All	All
Application	Xennobb	Xennobb	1.0.2	All	All	All
Application	Xennobb	Xennobb	1.0.3	All	All	All
Application	Xennobb	Xennobb	1.0.4	All	All	All
Application	Xennobb	Xennobb	1.0.5	All	All	All
Application	Xennobb	Xennobb	All	All	All	All

References

Reference	Source	Link	Tags
SurfiOnline	MISC	www.surfionline.com	Exploi

IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
SecurityReason - XennoBB <= "avatar gallery" Directory Transversal	SREASON	securityreason.com	
SecurityFocus	BUGTRAQ	www.securityfocus.com	
Secunia - Advisories - XennoBB "category" Parameter Directory Traversal Weakness	SECUNIA	secunia.com	Vendc
XennoBB Profile.PHP Directory Traversal Vulnerability	BID	www.securityfocus.com	Exploi
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**