



CVE-2012-1602

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

Summary

CVE	CVE-2012-1602
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-10-01 23:55:00 UTC
Updated	2012-10-02 04:00:00 UTC
Description	user.php in NextBBS 0.6 allows remote attackers to bypass authentication and gain administrator access by setting the use

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nextbbs	Nextbbs	0.6	All	All	All
Application	Nextbbs	Nextbbs	0.6	All	All	All

References

Reference	Source	Link	Tags
oss-security - Re: CVE-request: NextBBS 0.6.0 waraxe-2012-SA#080	MLIST	www.openwall.com	Exploit
[waraxe-2012-SA#080] - Multiple Vulnerabilities in NextBBS 0.6.0	MISC	www.waraxe.us	Exploit
80626	OSVDB	www.osvdb.org	
NextBBS Multiple Input Validation Security Vulnerabilities	BID	www.securityfocus.com	Exploit
20120327 [waraxe-2012-SA#080] - Multiple Vulnerabilities in NextBBS 0.6.0	BUGTRAQ	archives.neohapsis.com	Exploit
oss-security - CVE-request: NextBBS 0.6.0 waraxe-2012-SA#080	MLIST	www.openwall.com	Exploit
NextBBS 0.6.0 Authentication Bypass / SQL Injection / XSS ~ Packet Storm	MISC	packetstormsecurity.org	Exploit
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)