



# CVE-2010-4227

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

## Summary

<b>CVE</b>	CVE-2010-4227
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2011-02-25 19:00:00 UTC
<b>Updated</b>	2018-10-10 20:07:00 UTC
<b>Description</b>	The xdrDecodeString function in XNFS.NLM in Novell Netware 6.5 before SP8 allows remote attackers to cause a denial of

## Risk And Classification

### Problem Types: CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Novell	Netware	6.5	All	All	All
Application	Novell	Netware	6.5	sp1	All	All
Application	Novell	Netware	6.5	sp2	All	All
Application	Novell	Netware	6.5	sp3	All	All
Application	Novell	Netware	6.5	sp4	All	All
Application	Novell	Netware	6.5	sp5	All	All
Application	Novell	Netware	6.5	sp6	All	All
Application	Novell	Netware	6.5	All	All	All
Application	Novell	Netware	6.5	sp1	All	All
Application	Novell	Netware	6.5	sp2	All	All
Application	Novell	Netware	6.5	sp3	All	All
Application	Novell	Netware	6.5	sp4	All	All
Application	Novell	Netware	6.5	sp5	All	All
Application	Novell	Netware	6.5	sp6	All	All
Application	Novell	Netware	All	sp7	All	All

## References

Reference	Source	Link
IBM X-Force Exchange	XF	<a href="https://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="https://www.vupen.com">www.vupen.com</a>
Novell Netware 'XNFS.NLM' Component Remote Code Execution Vulnerability	BID	<a href="https://www.securityfocus.com/bid">www.securityfocus.com/bid</a>
NetWare XNFS Stack Overflow Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	<a href="https://www.securitytracker.com">www.securitytracker.com</a>
Novell Netware RPC XNFS xdrDecodeString Vulnerability - CXSecurity.com	SREASON	<a href="https://securityreason.com">securityreason.com</a>
Downloads - NetWare XNFS security updates	CONFIRM	<a href="https://download.novell.com">download.novell.com</a>
{PRL} Novell Netware RPC XNFS xdrDecodeString Remote Code Execution Vulnerability	MISC	<a href="https://www.protekresearch.com">www.protekresearch.com</a>
Zero Day Initiative	MISC	<a href="https://www.zerodayinitiative.com">www.zerodayinitiative.com</a>
Novell Netware XNFS.NLM "xdrDecodeString()" Buffer Overflow Vulnerability - Advisories - Community	SECUNIA	<a href="https://secunia.com">secunia.com</a>
SecurityFocus	BUGTRAQ	<a href="https://www.securityfocus.com">www.securityfocus.com</a>
Novell Netware RPC XNFS xdrDecodeString Vulnerability	EXPLOIT-DB	<a href="https://www.exploit-db.com">www.exploit-db.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.cve.org). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses/mitre).

**CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)**