



CVE-2015-2282

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2015-2282
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-06-02 14:59:00 UTC
Updated	2018-10-09 19:56:00 UTC
Description	Stack-based buffer overflow in the LZC decompression implementation (CsObjectInt::CsDecomprLZC function in vpa106cs

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	Gui	-	All	All	All
Application	Sap	Gui	-	All	All	All
Application	Sap	Maxdb	7.5	All	All	All
Application	Sap	Maxdb	7.6	All	All	All
Application	Sap	Maxdb	7.5	All	All	All
Application	Sap	Maxdb	7.6	All	All	All
Application	Sap	Netweaver Abap Application Server	-	All	All	All
Application	Sap	Netweaver Abap Application Server	-	All	All	All
Application	Sap	Netweaver Java Application Server	-	All	All	All
Application	Sap	Netweaver Java Application Server	-	All	All	All
Application	Sap	Netweaver Rfc Sdk	-	All	All	All
Application	Sap	Netweaver Rfc Sdk	-	All	All	All
Application	Sap	Rfc Library	All	All	All	All
Application	Sap	Rfc Library	All	All	All	All

References

Reference	Source	Link	Tags
-----------	--------	------	------

SecurityFocus	BUGTRAQ	www.securityfocus.com	
Full Disclosure: SAP Security Notes May 2015	FULLDISC	seclists.org	Exploit
SAP LZC/LZH Compression Denial Of Service ≈ Packet Storm	MISC	packetstormsecurity.com	Exploit
Multiple SAP Products Buffer Overflow and Denial of Service Vulnerabilities	BID	www.securityfocus.com	
Full Disclosure: [CORE-2015-0009] - SAP LZC/LZH Compression Multiple Vulnerabilities	FULLDISC	seclists.org	Exploit
SAP LZC/LZH Compression Multiple Vulnerabilities Advisory Core Security	MISC	www.coresecurity.com	Exploit
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

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