CVE-2012-2677

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2012-2677
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-07-25 19:55:00 UTC
Updated	2021-05-26 10:15:00 UTC
Description	Integer overflow in the ordered_malloc function in boost/pool/pool.hpp in Boost Pool before 3.9 makes it easier for context-d

Risk And Classification

Problem Types: CWE-189

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Boost	Pool	2.0.0	All	All	All
Application	Boost	Pool	2.0.0	All	All	All
Application	Boost	Pool	All	All	All	All

References

Reference	Source	Link	Tags
oss-security - Re: memory allocator upstream patches	MLIST	www.openwall.com	
oss-security - memory allocator upstream patches	MLIST	www.openwall.com	
Changeset 78326 – Boost C++ Libraries	CONFIRM	svn.boost.org	Exploit, Patch
Support / Security / Advisories / / MDVSA-2013:065 | Mandriva	MANDRIVA	www.mandriva.com	
[SECURITY] Fedora 17 Update: boost-1.48.0-13.fc17	FEDORA	lists.fedoraproject.org	
Memory allocator security revisited - Xi Wang	MISC	kqueue.org	
[SECURITY] Fedora 16 Update: boost-1.47.0-7.fc16	FEDORA	lists.fedoraproject.org	
Boost: Buffer overflow (GLSA 202105-04) — Gentoo security	GENTOO	security.gentoo.org	
#6701 (integer overflows in ordered_malloc()) – Boost C++ Libraries	CONFIRM	svn.boost.org	
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.

Legacy QID Mappings

20416 IBM DB2 Buffer Overflow Vulnerability (7145724)

710111 Gentoo Linux Boost Buffer overflow vulnerability (GLSA 202105-04)