CVE-2004-0601

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

Summary

CVE	CVE-2004-0601
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-12-23 05:00:00 UTC
Updated	2017-07-11 01:30:00 UTC
Description	distcc before 2.16, when running on 64-bit platforms, does not interpret IP-based access control rules correctly, which coulc

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Distcc	Distcc	2.10	All	All	All
Application	Distcc	Distcc	2.11	All	All	All
Application	Distcc	Distcc	2.12	All	All	All
Application	Distcc	Distcc	2.13	All	All	All
Application	Distcc	Distcc	2.14	All	All	All
Application	Distcc	Distcc	2.15	All	All	All
Application	Distcc	Distcc	2.7	All	All	All
Application	Distcc	Distcc	2.9	All	All	All
Application	Distcc	Distcc	2.10	All	All	All
Application	Distcc	Distcc	2.11	All	All	All
Application	Distcc	Distcc	2.12	All	All	All
Application	Distcc	Distcc	2.13	All	All	All
Application	Distcc	Distcc	2.14	All	All	All
Application	Distcc	Distcc	2.15	All	All	All
Application	Distcc	Distcc	2.7	All	All	All
Application	Distcc	Distcc	2.9	All	All	All

References

Reference	Source	Link	Tags
distcc · GitHub	CONFIRM	distcc.samba.org	Vendor Adviso
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
'distcc' Access Control Bypass Vulnerability	BID	www.securityfocus.com	Patch, Vendor
Secunia - Advisories - distcc IP-based Access Control Rules Security Bypass	SECUNIA	secunia.com	Patch, Vendor
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

No vendor comments have been submitted for this CVE.

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