CVE-2015-5986

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

Summary

CVE	CVE-2015-5986
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-09-05 02:59:00 UTC
Updated	2016-12-31 02:59:00 UTC
Description	openpgpkey_61.c in named in ISC BIND 9.9.7 before 9.9.7-P3 and 9.10.x before 9.10.2-P4 allows remote attackers to caus

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Mac Os X Server	5.0.15	All	All	All
Operating System	Apple	Mac Os X Server	5.0.15	All	All	All
Application	Isc	Bind	All	p3	All	All
Application	Isc	Bind	All	p2	All	All

References

Reference
BIND 9.10.3 Release Notes | Internet Systems Consortium Knowledge Base
404 Page not found
[SECURITY] Fedora 22 Update: bind99-9.9.7-7.P3.fc22
CVE-2015-5986: An incorrect boundary check can trigger a REQUIRE assertion failure in openpgpkey_61.c | Internet Systems Consortium Kr
[SECURITY] Fedora 23 Update: bind99-9.9.7-7.P3.fc23
McAfee KnowledgeBase - Intel Security - Security Bulletin: Firewall Enterprise update fixes BIND CVE-2015-5722 and CVE-2015-5986 vulner
BIND: Denial of Service (GLSA 201510-01) — Gentoo Security
BIND 9.9.8-S1 Release Notes | Internet Systems Consortium Knowledge Base
ISC BIND 'openpgpkey_61.c' Remote Denial of Service Vulnerability
About the security content of OS X Server 5.0.15 - Apple Support

BIND 9.9.8 Release Notes | Internet Systems Consortium Knowledge Base
September 2015 ISC BIND Vulnerabilities in NetApp Products | NetApp Product Security
APPLE-SA-2015-10-21-8 OS X Server 5.0.15
BIND OpenPGP Key Processing Flaw Lets Remote Users Cause the Target DNS Service to Terminate - SecurityTracker
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**