CVE-2018-5745

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-5745
State	PUBLIC
Assigner	security-officer@isc.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-10-09 16:15:00 UTC
Updated	2019-11-06 01:15:00 UTC
Description	"managed-keys" is a feature which allows a BIND resolver to automatically maintain the keys used by trust anchors which c

Risk And Classification

Problem Types: CWE-327

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Isc	Bind	9.10.7	-	All	All
Application	Isc	Bind	9.10.8	p1	All	All
Application	Isc	Bind	9.11.5	-	All	All
Application	Isc	Bind	9.11.5	p1	All	All
Application	Isc	Bind	9.11.5	s3	All	All
Application	Isc	Bind	9.12.3	-	All	All
Application	Isc	Bind	9.12.3	p1	All	All
Application	Isc	Bind	9.9.3	s1	All	All
Application	Isc	Bind	9.10.7	-	All	All
Application	Isc	Bind	9.10.8	p1	All	All
Application	Isc	Bind	9.11.5	-	All	All
Application	Isc	Bind	9.11.5	p1	All	All
Application	Isc	Bind	9.11.5	s3	All	All
Application	Isc	Bind	9.12.3	-	All	All
Application	Isc	Bind	9.12.3	p1	All	All
Application	Isc	Bind	9.9.3	s1	All	All
Application	Isc	Bind	All	All	All	All

Application	Isc	Bind	All	All	All	All
Application	Isc	Bind	All	All	All	All
Application	Isc	Bind	All	All	All	All

References

Reference
Red Hat Customer Portal
CVE-2018-5745: An assertion failure can occur if a trust anchor rolls over to an unsupported key algorithm when using managed-keys - Secur
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 296087 Oracle Solaris 11.4 Support Repository Update (SRU) 8.1.5 Missing (CPUAPR2019)
- 377284 Alibaba Cloud Linux Security Update for bind (ALINUX2-SA-2020:0083)
- 500052 Alpine Linux Security Update for bind
- 503733 Alpine Linux Security Update for bind