CVE-2020-8625

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-8625
State	PUBLIC
Assigner	security-officer@isc.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-02-17 23:15:00 UTC
Updated	2023-11-07 03:26:00 UTC
Description	BIND servers are vulnerable if they are running an affected version and are configured to use GSS-TSIG features. In a cont

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Isc	Bind	9.11.21	s1	All	All
Application	Isc	Bind	9.11.27	s1	All	All
Application	Isc	Bind	9.11.3	s1	All	All
Application	Isc	Bind	9.11.5	s3	All	All
Application	Isc	Bind	9.11.5	s5	All	All
Application	Isc	Bind	9.11.6	s1	All	All
Application	Isc	Bind	9.11.7	s1	All	All
Application	Isc	Bind	9.11.8	s1	All	All

Application	Isc	Bind	9.16.11	s1	All	All
Application	Isc	Bind	9.16.8	s1	All	All
Application	Isc	Bind	9.17.0	All	All	All
Application	Isc	Bind	9.17.1	All	All	All
Application	Isc	Bind	9.11.21	s1	All	All
Application	Isc	Bind	9.11.27	s1	All	All
Application	Isc	Bind	9.11.3	s1	All	All
Application	Isc	Bind	9.11.5	s3	All	All
Application	Isc	Bind	9.11.5	s5	All	All
Application	Isc	Bind	9.11.6	s1	All	All
Application	Isc	Bind	9.11.7	s1	All	All
Application	Isc	Bind	9.11.8	s1	All	All
Application	Isc	Bind	9.16.11	s1	All	All
Application	Isc	Bind	9.16.8	s1	All	All
Application	Isc	Bind	9.17.0	All	All	All
Application	Isc	Bind	9.17.1	All	All	All
Application	Isc	Bind	All	All	All	All
Application	Isc	Bind	All	All	All	All
Hardware	Netapp	500f	-	All	All	All
Operating System	Netapp	500f Firmware	-	All	All	All
Hardware	Netapp	A250	-	All	All	All
Operating System	Netapp	A250 Firmware	-	All	All	All
Application	Netapp	Cloud Backup	-	All	All	All
Application	Siemens	Sinec Infrastructure Network Services	All	All	All	All

References

Reference
[SECURITY] Fedora 32 Update: bind-9.11.28-1.fc32 - package-announce - Fedora Mailing-Lists
CVE-2020-8625: A vulnerability in BIND's GSSAPI security policy negotiation can be targeted by a buffer overflow attack - Security Advisories
oss-security - BIND Operational Notification: Enabling the new BIND option "stale-answer-client-timeout" can result in unexpected server termi
[SECURITY] Fedora 33 Update: bind-9.11.28-1.fc33 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 32 Update: bind-9.11.28-1.fc32 - package-announce - Fedora Mailing-Lists
ZDI-21-195 | Zero Day Initiative
[SECURITY] [DLA 2568-1] bind9 security update
[SECURITY] Fedora 34 Update: bind-9.16.11-5.fc34 - package-announce - Fedora Mailing-Lists

cert-portal.siemens.com/productcert/pdf/ssa-389290.pdf

[SECURITY] Fedora 33 Update: bind-9.11.28-1.fc33 - package-announce - Fedora Mailing-Lists

oss-security - BIND Operational Notification: Zone journal (.jnl) file incompatibility,after upgrading to BIND 9.16.12 and 9.17

CVE-2020-8625 ISC BIND Vulnerability in NetApp Products | NetApp Product Security

[SECURITY] Fedora 34 Update: bind-9.16.11-5.fc34 - package-announce - Fedora Mailing-Lists

Debian -- Security Information -- DSA-4857-1 bind9

CVE Program record

NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

LEGACY: ISC would like to thank an anonymous party, working in conjunction with Trend Micro Zero Day Initiative, for reporting this issue to us.

Legacy QID Mappings

281600 Fedora Security Update for bind (FEDORA-2021-8b4744f152)

281607 Fedora Security Update for bind (FEDORA-2021-0595625865)

281608 Fedora Security Update for bind (FEDORA-2021-28f97e232d)

296069 Oracle Solaris 11.4 Support Repository Update (SRU) 31.88.5 Missing (CPUJAN2021)

352243 Amazon Linux Security Advisory for bind: ALAS-2021-1485

352252 Amazon Linux Security Advisory for bind: ALAS2-2021-1614

376869 Alibaba Cloud Linux Security Update for bind (ALINUX2-SA-2021:0011)

377151 Alibaba Cloud Linux Security Update for bind (ALINUX3-SA-2021:0025)

500059 Alpine Linux Security Update for bind

503739 Alpine Linux Security Update for bind

670330 EulerOS Security Update for bind (EulerOS-SA-2021-1894)

670359 EulerOS Security Update for bind (EulerOS-SA-2021-1865)

670364 EulerOS Security Update for bind (EulerOS-SA-2021-1766)

670386 EulerOS Security Update for bind (EulerOS-SA-2021-1939)

670431 EulerOS Security Update for bind (EulerOS-SA-2021-1918)

670596 EulerOS Security Update for bind (EulerOS-SA-2021-2354)

730228 McAfee Web Gateway Multiple Vulnerabilities (WP-3445, WP-3483, WP-3527, WP-3528, WP-3547, WP-3584,WP-3589,WP-

3611)

750333 OpenSUSE Security Update for bind (openSUSE-SU-2021:0375-1)

900065 CBL-Mariner Linux Security Update for bind 9.16.3

903172 Common Base Linux Mariner (CBL-Mariner) Security Update for bind (3907)

940192 AlmaLinux Security Update for bind (ALSA-2021:0670)