CVE-2020-1472

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-1472
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-08-17 19:15:00 UTC
Updated	2024-01-19 00:15:00 UTC
Description	An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection

Risk And Classification

EPSS: 0.943800000 probability, percentile 0.999690000 (date 2026-04-01)

CISA KEV: Listed on 2021-11-03; due 2022-05-03; ransomware use Known

Problem Types: CWE-330

CISA Known Exploited Vulnerability

Vendor	Microsoft
Product	Netlogon
Name	Microsoft Netlogon Privilege Escalation Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	Reference CISA's ED 20-04 (https://www.cisa.gov/news-events/directives/ed-20-04-mitigate-netlogon-elevation-privilege-vulnerability-august-2020-patch-tuesday) for further guidance and requirements. Note: The due date for addressing this vulnerability aligns with the requirements outlined in ED 20-04. https://nvd.nist.gov/vuln/detail/CVE-2020-1472

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All

Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2012	-	All	All	All
Operating System	Microsoft	Windows Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Server 2012	-	All	All	All
Operating System	Microsoft	Windows Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Server 2016	-	All	All	All
Operating System	Microsoft	Windows Server 2016	1903	All	All	All
Operating System	Microsoft	Windows Server 2016	1909	All	All	All
Operating System	Microsoft	Windows Server 2016	2004	All	All	All
Operating System	Microsoft	Windows Server 2016	-	All	All	All
Operating System	Microsoft	Windows Server 2016	1903	All	All	All
Operating System	Microsoft	Windows Server 2016	1909	All	All	All
Operating System	Microsoft	Windows Server 2016	2004	All	All	All
Operating System	Microsoft	Windows Server 2019	-	All	All	All
Operating System	Microsoft	Windows Server 2019	-	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Application	Oracle	Zfs Storage Appliance Kit	8.8	All	All	All
Application	Samba	Samba	All	All	All	All
Application	Samba	Samba	All	All	All	All
Application	Synology	Directory Server	All	All	All	All
Application	Synology	Directory Server	All	All	All	All

References

Reference	Source	Link

[security-announce] openSUSE-SU-2020:1526-1: important: Security update	SUSE	lists.ope
oss-security - Samba and CVE-2020-1472 ("Zerologon")	MLIST	www.op
[SECURITY] Fedora 32 Update: samba-4.12.7-0.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fed
[security-announce] openSUSE-SU-2020:1513-1: important: Security update	SUSE	lists.ope
[SECURITY] Fedora 33 Update: samba-4.13.0-11.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fed
Zerologon Proof Of Concept ≈ Packet Storm	MISC	packets
[SECURITY] Fedora 31 Update: samba-4.11.13-0.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fed
USN-4510-1: Samba vulnerability | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubu
USN-4559-1: Samba update | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubu
USN-4510-2: Samba vulnerability | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubu
VU#490028 - Microsoft Windows Netlogon Remote Protocol (MS-NRPC) uses insecure AES-CFB8 initialization vector	CERT-VN	www.kb
N/A	N/A	portal.m
[SECURITY] Fedora 33 Update: samba-4.13.0-11.fc33 - package-announce - Fedora Mailing-Lists		lists.fed
Samba: Multiple vulnerabilities (GLSA 202012-24) — Gentoo security	GENTOO	security
[SECURITY] Fedora 31 Update: samba-4.11.13-0.fc31 - package-announce - Fedora Mailing-Lists		lists.fed
[SECURITY] Fedora 32 Update: samba-4.12.7-0.fc32 - package-announce - Fedora Mailing-Lists		lists.fed
Zerologon Netlogon Privilege Escalation ≈ Packet Storm	MISC	packets
Synology Inc.	CONFIRM	www.sy
[SECURITY] [DLA 2463-1] samba security update	MLIST	lists.deb
Oracle Critical Patch Update Advisory - April 2021	MISC	www.or
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist
CISA Known Exploited Vulnerabilities catalog	CISA	www.cis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 159201 Oracle Enterprise Linux Security Update for samba (ELSA-2021-1647)
- 239322 Red Hat Update for samba (RHSA-2021:1647)
- 239759 Red Hat Update for samba security (RHSA-2021:3723)
- 352379 Amazon Linux Security Advisory for samba: ALAS2-2021-1649
- 374349 McAfee Web Gateway Privilege Escalation Vulnerability (KB93377)
- 377403 Alibaba Cloud Linux Security Update for samba (ALINUX3-SA-2021:0077)
- 377458 Alibaba Cloud Linux Security Update for samba (ALINUX2-SA-2020:0196)

377458 Alibaba Cloud Linux Security Update for samba (ALINUX2-SA-2020:0196)

500629 Alpine Linux Security Update for samba

504389 Alpine Linux Security Update for samba

670878 EulerOS Security Update for samba (EulerOS-SA-2021-1118)

670882 EulerOS Security Update for samba (EulerOS-SA-2020-2396)

750630 OpenSUSE Security Update for samba (openSUSE-SU-2020:1526-1)

901685 Common Base Linux Mariner (CBL-Mariner) Security Update for samba (7350)

906954 Common Base Linux Mariner (CBL-Mariner) Security Update for samba (7350-1)

940102 AlmaLinux Security Update for samba (ALSA-2021:1647)

960808 Rocky Linux Security Update for samba (RLSA-2021:1647)