CVE-2021-23017

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-23017
State	PUBLIC
Assigner	f5sirt@f5.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-06-01 13:15:00 UTC
Updated	2023-11-07 03:30:00 UTC
Description	A security issue in nginx resolver was identified, which might allow an attacker who is able to forge UDP packets from the D

Risk And Classification

Problem Types: CWE-193

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	F5	Nginx	All	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Application	Netapp	Ontap Select Deploy Administration Utility	-	All	All	All
Application	Nginx	Nginx	All	All	All	All
Application	Openresty	Openresty	All	All	All	All
Application	Oracle	Blockchain Platform	All	All	All	All
Application	Oracle	Communications Control Plane Monitor	3.4	All	All	All
Application	Oracle	Communications Control Plane Monitor	4.2	All	All	All
Application	Oracle	Communications Control Plane Monitor	4.3	All	All	All
Application	Oracle	Communications Control Plane Monitor	4.4	All	All	All
Application	Oracle	Communications Fraud Monitor	All	All	All	All
Application	Oracle	Communications Operations Monitor	3.4	All	All	All
Application	Oracle	Communications Operations Monitor	4.2	All	All	All
Application	Oracle	Communications Operations Monitor	4.3	All	All	All
Application	Oracle	Communications Operations Monitor	4.4	All	All	All
Application	Oracle	Communications Session Border Controller	8.4	All	All	All

Application	Oracle	Communications Session Border Controller	9.0	All	All	All
Application	Oracle	Enterprise Communications Broker	3.3.0	All	All	All
Application	Oracle	Enterprise Session Border Controller	8.4	All	All	All
Application	Oracle	Enterprise Session Border Controller	9.0	All	All	All
Application	Oracle	Enterprise Telephony Fraud Monitor	3.4	All	All	All
Application	Oracle	Enterprise Telephony Fraud Monitor	4.2	All	All	All
Application	Oracle	Enterprise Telephony Fraud Monitor	4.3	All	All	All
Application	Oracle	Enterprise Telephony Fraud Monitor	4.4	All	All	All
Application	Oracle	Goldengate	All	All	All	All

References

Reference
support.f5.com/csp/article/K12331123,
Pony Mail!
Pony Mail!
[apisix-notifications] 20210607 [GitHub] [apisix-website] Serendipity96 opened a new pull request #362: feat: add new blog
Pony Mail!
Oracle Critical Patch Update Advisory - April 2022
Pony Mail!
[SECURITY] Fedora 34 Update: nginx-1.20.1-2.fc34 - package-announce - Fedora Mailing-Lists
support.f5.com/csp/article/K12331123%2C
[SECURITY] Fedora 33 Update: nginx-1.20.1-2.fc33 - package-announce - Fedora Mailing-Lists
Pony Mail!
Oracle Critical Patch Update Advisory - October 2021
[apisix-notifications] 20210608 [GitHub] [apisix-website] netlify[bot] edited a comment on pull request #362: docs: added "Apache APISIX not a
CVE-2021-23017 NGINX Vulnerability in NetApp Products | NetApp Product Security
[apisix-notifications] 20210608 [apisix-website] branch master updated: docs: added "Apache APISIX not affected by NGINX CVE-2021-23017
Oracle Critical Patch Update Advisory - January 2022
[nginx-announce] nginx security advisory (CVE-2021-23017)
[SECURITY] Fedora 34 Update: nginx-1.20.1-2.fc34 - package-announce - Fedora Mailing-Lists
Nginx 1.20.0 Denial Of Service ≈ Packet Storm
[apisix-notifications] 20210608 [GitHub] [apisix-website] liuxiran merged pull request #362: docs: added "Apache APISIX not affected by NGIN
[apisix-notifications] 20210608 [GitHub] [apisix-website] liuxiran commented on a change in pull request #362: docs: added "Apache APISIX n
[SECURITY] Fedora 33 Update: nginx-1.20.1-2.fc33 - package-announce - Fedora Mailing-Lists
CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159245 Oracle Enterprise Linux Security Update for nginx:1.18 (ELSA-2021-2259)

159255 Oracle Enterprise Linux Security Update for nginx:1.16 (ELSA-2021-2290)

159606 Oracle Enterprise Linux Security Update for nginx:1.20 (ELSA-2022-0323)

178609 Debian Security Update for nginx (DLA 2670-1)

178620 Debian Security Update for nginx (DSA 4921-1)

178635 Debian Security Update for nginx (DSA 4921-1)

179575 Debian Security Update for nginx (CVE-2021-23017)

198386 Ubuntu Security Notification for nginx vulnerability (USN-4967-1)

239362 Red Hat Update for rh-nginx118-nginx (RHSA-2021:2258)

239412 Red Hat Update for nginx:1.16 (RHSA-2021:2290)

239415 Red Hat Update for rh-nginx116-nginx (RHSA-2021:2278)

239419 Red Hat Update for nginx:1.18 (RHSA-2021:2259)

239420 Red Hat Update for rh-nginx118-nginx (RHSA-2021:2258)

239445 Red Hat Update for rh-nginx116-nginx (RHSA-2021:2278)

239446 Red Hat Update for rh-nginx118-nginx (RHSA-2021:2258)

240048 Red Hat Update for nginx:1.20 (RHSA-2022:0323)

281627 Fedora Security Update for nginx (FEDORA-2021-393d698493)

281628 Fedora Security Update for nginx (FEDORA-2021-b37cffac0d)

352378 Amazon Linux Security Advisory for nginx: ALAS-2021-1507

352820 Amazon Linux Security Advisory for nginx: AL2012-2021-344

356196 Amazon Linux Security Advisory for nginx : ALASNGINX1-2023-003

377103 Alibaba Cloud Linux Security Update for nginx:1.20 (ALINUX3-SA-2022:0016)

377116 Alibaba Cloud Linux Security Update for nginx:1.18 (ALINUX3-SA-2021:0036)

500429 Alpine Linux Security Update for nginx

501443 Alpine Linux Security Update for nginx

501757 Alpine Linux Security Update for nginx

504188 Alpine Linux Security Update for nginx

670550 EulerOS Security Update for nginx (EulerOS-SA-2021-2308)

670582 EulerOS Security Update for nginx (EulerOS-SA-2021-2340)

670654 EulerOS Security Update for nginx (EulerOS-SA-2021-2412)

671013 EulerOS Security Update for nginx (EulerOS-SA-2021-2599)

690131 Free Berkeley Software Distribution (FreeBSD) Security Update for nginx (0882f019-bd60-11eb-9bdd-8c164567ca3c)

710076 Gentoo Linux nginx Remote code execution (GLSA 202105-38)

730096 Nginx Arbitrary Code Execution Vulnerability

750054 SUSE Enterprise Linux Security Update for nginx (SUSE-SU-2021:1792-1)

750083 SUSE Enterprise Linux Security Update for nginx (SUSE-SU-2021:1815-1)

750084 SUSE Enterprise Linux Security Update for nginx (SUSE-SU-2021:1814-1)

750095 SUSE Enterprise Linux Security Update for nginx (SUSE-SU-2021:1839-1)

750175 OpenSUSE Security Update for nginx (openSUSE-SU-2021:0835-1)

750793 OpenSUSE Security Update for nginx (openSUSE-SU-2021:1815-1)

900026 CBL-Mariner Linux Security Update for nginx 1.16.1

902844 Common Base Linux Mariner (CBL-Mariner) Security Update for nginx (4337)

940197 AlmaLinux Security Update for nginx:1.18 (ALSA-2021:2259)

940229 AlmaLinux Security Update for nginx:1.16 (ALSA-2021:2290)

940441 AlmaLinux Security Update for nginx:1.20 (ALSA-2022:0323)

960037 Rocky Linux Security Update for nginx:1.18 (RLSA-2021:2259)

960097 Rocky Linux Security Update for nginx:1.16 (RLSA-2021:2290)

960781 Rocky Linux Security Update for nginx:1.20 (RLSA-2022:0323)

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