CVE-2020-14343

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-14343
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-02-09 21:15:00 UTC
Updated	2023-07-06 18:15:00 UTC
Description	A vulnerability was discovered in the PyYAML library in versions before 5.4, where it is susceptible to arbitrary code executi

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	La
Application	Oracle	Communications Cloud Native Core Network Function Cloud Native Environment	1.10.0	All	All	All
Application	Oracle	Communications Cloud Native Core Network Function Cloud Native Environment	22.1.0	All	All	All
Application	Pyyaml	Pyyaml	All	All	All	All
Application	Pyyaml	Pyyaml	All	All	All	All

References

Reference	Source	Link	Tags
Oracle Critical Patch Update Advisory - April 2022	MISC	www.oracle.com	
Resolve CVE for PyYAML - CVE-2020-14343 · Issue #2252 · SeldonIO/seldon-core · GitHub	CONFIRM	github.com	
.load() and FullLoader still vulnerable to fairly trivial RCE · Issue #420 · yaml/pyyaml · GitHub	MISC	github.com	
1860466 – (CVE-2020-14343) CVE-2020-14343 PyYAML: incomplete fix for CVE-2020-1747	MISC	bugzilla.redhat.com	Issue Trac
Oracle Critical Patch Update Advisory - July 2022	N/A	www.oracle.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159289 Oracle Enterprise Linux Security Update for python38:3.8 and python38-devel:3.8 (ELSA-2021-2583)

198358 Ubuntu Security Notification for PyYAML vulnerability (USN-4940-1)

239464 Red Hat Update for python38:3.8 and python38-devel:3.8 (RHSA-2021:2583)

239895 Red Hat Update for Satellite 6.10 (RHSA-2021:4702)

296067 Oracle Solaris 11.4 Support Repository Update (SRU) 33.94.0 Missing (CPUAPR2021)

378427 Oracle PeopleSoft Enterprise PeopleTools Product Multiple Vulnerabilities (CPUAPR2023)

500784 Alpine Linux Security Update for py3-yaml

501479 Alpine Linux Security Update for py3-yaml

501772 Alpine Linux Security Update for py3-yaml

504337 Alpine Linux Security Update for py3-yaml

670312 EulerOS Security Update for PyYAML (EulerOS-SA-2021-1912)

670367 EulerOS Security Update for PyYAML (EulerOS-SA-2021-1958)

670388 EulerOS Security Update for PyYAML (EulerOS-SA-2021-1937)

690117 Free Berkeley Software Distribution (FreeBSD) Security Update for pyyaml (c7ec6375-c3cf-11eb-904f-14dae9d5a9d2)

710880 Gentoo Linux PyYAML Arbitrary Code Execution Vulnerability (GLSA 202402-33)

751033 SUSE Enterprise Linux Security Update for python-PyYAML (SUSE-SU-2021:2818-1)

752486 SUSE Enterprise Linux Security Update for python-PyYAML (SUSE-SU-2022:2841-1)

904855 Common Base Linux Mariner (CBL-Mariner) Security Update for mozjs60 (12376)

904900 Common Base Linux Mariner (CBL-Mariner) Security Update for PyYAML (12296)

905102 Common Base Linux Mariner (CBL-Mariner) Security Update for PyYAML (12456)

907556 Common Base Linux Mariner (CBL-Mariner) Security Update for PyYAML (31782-1)

940207 AlmaLinux Security Update for python38:3.8 and python38-devel:3.8 (ALSA-2021:2583)

960084 Rocky Linux Security Update for python38:3.8 and python38-devel:3.8 (RLSA-2021:2583)

980646 Python (pip) Security Update for PyYAML (GHSA-8q59-q68h-6hv4)

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

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