CVE-2022-37454

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-37454
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-10-21 06:15:00 UTC
Updated	2023-05-03 11:15:00 UTC
Description	The Keccak XKCP SHA-3 reference implementation before fdc6fef has an integer overflow and resultant buffer overflow tha

Risk And Classification

Problem Types: CWE-190

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	11.0	All	All	All
Application	Extended Keccak Code Package Project	Extended Keccak Code Package	-	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Application	Php	Php	All	All	All	All
Application	Pypy	Pypy	All	All	All	All
Application	Pysha3 Project	Pysha3	All	All	All	All
Application	Python	Python	All	All	All	All
Application	Sha3 Project	Sha3	All	All	All	All

References

Reference	Source	Link	T
SHA-3 Buffer Overflow – Nicky Mouha	MISC	mouha.be	
[SECURITY] [DLA 3175-1] python3.7 security update	MLIST	lists.debian.org	
Debian -- Security Information -- DSA-5267-1 pysha3	DEBIAN	www.debian.org	
[SECURITY] Fedora 36 Update: php-8.1.12-1.fc36 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject.org	

SHA-3 Buffer Overflow | Hacker News	MISC	news.ycombinator.com
A Vulnerability in Implementations of SHA-3, SHAKE, EdDSA, and Other NIST-Approved Algorithm	MISC	eprint.iacr.org
Buffer overflow in sponge queue functions · Advisory · XKCP/XKCP · GitHub	MISC	github.com
[SECURITY] [DLA 3174-1] pysha3 security update	MLIST	lists.debian.org
A Vulnerability in Implementations of SHA-3, Shake, EdDSA | Hacker News	MISC	news.ycombinator.com
[SECURITY] Fedora 36 Update: php-8.1.12-1.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
Debian -- Security Information -- DSA-5269-1 pypy3	DEBIAN	www.debian.org
[SECURITY] Fedora 35 Update: php-8.0.25-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 35 Update: php-8.0.25-1.fc35 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject.org
Python, PyPy3: Multiple Vulnerabilities (GLSA 202305-02) — Gentoo security	MISC	security.gentoo.org
Hash Functions | CSRC	MISC	csrc.nist.gov
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 150663 PHP Buffer Overflow Vulnerability (CVE-2022-37454)
- 160478 Oracle Enterprise Linux Security Update for php:8.0 (ELSA-2023-0848)
- 160486 Oracle Enterprise Linux Security Update for Hypertext Preprocessor (PHP) (ELSA-2023-0965)
- 160592 Oracle Enterprise Linux Security Update for 8.1 (ELSA-2023-2417)
- 160672 Oracle Enterprise Linux Security Update for php:7.4 (ELSA-2023-2903)
- 181181 Debian Security Update for pysha3 (DSA 5267-1)
- 181182 Debian Security Update for pysha3 (DLA 3174-1)
- 181183 Debian Security Update for python3.7 (DLA 3175-1)
- 181185 Debian Security Update for pypy3 (DSA 5269-1)
- 181210 Debian Security Update for php7.4 (DSA 5277-1)
- 181332 Debian Security Update for php7.3 (DLA 3243-1)
- 183958 Debian Security Update for pypy3 (CVE-2022-37454)
- 199021 Ubuntu Security Notification for Hypertext Preprocessor (PHP) Vulnerabilities (USN-5717-1)
- 199068 Ubuntu Security Notification for Python Vulnerabilities (USN-5767-1)

199219 Ubuntu Security Notification for Python Vulnerability (USN-5767-3)

199497 Ubuntu Security Notification for Python Vulnerabilities (USN-5888-1)

199505 Ubuntu Security Notification for Python Vulnerability (USN-5931-1)

199536 Ubuntu Security Notification for Python Vulnerability (USN-5930-1)

199962 Ubuntu Security Notification for pysha3 Vulnerability (USN-6525-1)

199968 Ubuntu Security Notification for PyPy Vulnerability (USN-6524-1)

20342 Oracle Database 21c Critical Patch Update - April 2023

241205 Red Hat Update for php:8.0 (RHSA-2023:0848)

241219 Red Hat Update for Hypertext Preprocessor (PHP) (RHSA-2023:0965)

241447 Red Hat Update for php:8.1 (RHSA-2023:2417)

241540 Red Hat Update for php:7.4 (RHSA-2023:2903)

283268 Fedora Security Update for Hypertext Preprocessor (PHP) (FEDORA-2022-f2a5082860)

283279 Fedora Security Update for Hypertext Preprocessor (PHP) (FEDORA-2022-1ecc10276e)

283330 Fedora Security Update for python3.6 (FEDORA-2022-004b185fa4)

283331 Fedora Security Update for python3.6 (FEDORA-2022-104076b1d8)

283336 Fedora Security Update for python3.8 (FEDORA-2022-7798bf3aa3)

283343 Fedora Security Update for python3.7 (FEDORA-2022-385d2ea041)

283344 Fedora Security Update for python3.8 (FEDORA-2022-5fd3e7f635)

283345 Fedora Security Update for python3.7 (FEDORA-2022-760d1eac9b)

283418 Fedora Security Update for python3.7 (FEDORA-2022-4f547d1cc6)

283419 Fedora Security Update for python3.8 (FEDORA-2022-cb47d98a05)

283426 Fedora Security Update for python3.6 (FEDORA-2022-cae8089f93)

283450 Fedora Security Update for Hypertext Preprocessor (PHP) (FEDORA-2022-f204e1d0ed)

283597 Fedora Security Update for pypy3.8 (FEDORA-2023-78b4ce2f23)

283600 Fedora Security Update for pypy3.9 (FEDORA-2023-af5206f71d)

283601 Fedora Security Update for pypy3.8 (FEDORA-2023-943556a733)

283604 Fedora Security Update for pypy3.9 (FEDORA-2023-097dd40685)

283797 Fedora Security Update for pypy3.7 (FEDORA-2023-930077c742)

284294 Fedora Security Update for python3.7 (FEDORA-2022-792bd23738)

284295 Fedora Security Update for python3.8 (FEDORA-2022-eda83be115)

284296 Fedora Security Update for python3.6 (FEDORA-2022-17bc21cf38)

296098 Oracle Solaris 11.4 Support Repository Update (SRU) 52.132.2 Missing (CPUOCT2022)

354125 Amazon Linux Security Advisory for python3 : ALAS2-2022-1897

354247 Amazon Linux Security Advisory for python38 : ALAS-2022-1651

354258 Amazon Linux Security Advisory for python36 : ALAS-2022-1652

354414 Amazon Linux Security Advisory for php8.1 : ALAS2022-2022-243

354548 Amazon Linux Security Advisory for php8.1 : ALAS-2022-243

355222 Amazon Linux Security Advisory for php8.1 : ALAS2023-2023-081

356067 Amazon Linux Security Advisory for Hypertext Preprocessor (PHP) : ALASPHP8.1-2023-001

356071 Amazon Linux Security Advisory for Hypertext Preprocessor (PHP) : ALASPHP8.0-2023-004

356079 Amazon Linux Security Advisory for Hypertext Preprocessor (PHP) : ALASPHP8.1-2023-001

356091 Amazon Linux Security Advisory for Hypertext Preprocessor (PHP) : ALAS2PHP8.0-2023-004

356253 Amazon Linux Security Advisory for python38 : ALASPYTHON3.8-2023-004

356490 Amazon Linux Security Advisory for python38 : ALAS2PYTHON3.8-2023-004

378747 Alibaba Cloud Linux Security Update for php:7.4 (ALINUX3-SA-2023:0088)

38880 Hypertext Preprocessor (PHP) Multiple Security Vulnerabilities (81738, 81739)

502574 Alpine Linux Security Update for php8

502576 Alpine Linux Security Update for php8

502577 Alpine Linux Security Update for php81

502593 Alpine Linux Security Update for php7

502608 Alpine Linux Security Update for python3

503213 Alpine Linux Security Update for php82

503679 Alpine Linux Security Update for php7

504338 Alpine Linux Security Update for python3

505229 Alpine Linux Security Update for php81

506153 Alpine Linux Security Update for php82

672594 EulerOS Security Update for python3 (EulerOS-SA-2023-1334)

672601 EulerOS Security Update for Hypertext Preprocessor (PHP) (EulerOS-SA-2023-1332)

672618 EulerOS Security Update for python3 (EulerOS-SA-2023-1368)

672659 EulerOS Security Update for python3 (EulerOS-SA-2023-1396)

672704 EulerOS Security Update for python3 (EulerOS-SA-2023-1455)

672783 EulerOS Security Update for python3 (EulerOS-SA-2023-1480)

710684 Gentoo Linux Hypertext Preprocessor (PHP) Multiple Vulnerabilities (GLSA 202211-03)

710714 Gentoo Linux Python, PyPy3 Multiple Vulnerabilities (GLSA 202305-02)

752779 SUSE Enterprise Linux Security Update for python3 (SUSE-SU-2022:3924-1)

752863 SUSE Enterprise Linux Security Update for php7 (SUSE-SU-2022:3997-1)

752878 SUSE Enterprise Linux Security Update for php7 (SUSE-SU-2022:4067-1)

752898 SUSE Enterprise Linux Security Update for php7 (SUSE-SU-2022:4069-1)

752901 SUSE Enterprise Linux Security Update for php74 (SUSE-SU-2022:4068-1)

752927 SUSE Enterprise Linux Security Update for php8 (SUSE-SU-2022:4005-1)

752940 SUSE Enterprise Linux Security Update for python3 (SUSE-SU-2022:4274-1)

752957 SUSE Enterprise Linux Security Update for python3 (SUSE-SU-2022:4281-1)

753766 SUSE Enterprise Linux Security Update for python39 (SUSE-SU-2023:0707-1)

904576 Common Base Linux Mariner (CBL-Mariner) Security Update for python3 (11507)

904579 Common Base Linux Mariner (CBL-Mariner) Security Update for python3 (11503)

904585 Common Base Linux Mariner (CBL-Mariner) Security Update for Hypertext Preprocessor (PHP) (11501)

904634 Common Base Linux Mariner (CBL-Mariner) Security Update for Hypertext Preprocessor (PHP) (11501-1)

904721 Common Base Linux Mariner (CBL-Mariner) Security Update for python3 (11503-1)

904739 Common Base Linux Mariner (CBL-Mariner) Security Update for python3 (11507-1)

940930 AlmaLinux Security Update for php:8.0 (ALSA-2023:0848)

940947 AlmaLinux Security Update for Hypertext Preprocessor (PHP) (ALSA-2023:0965)

941025 AlmaLinux Security Update for php:8.1 (ALSA-2023:2417)

941091 AlmaLinux Security Update for php:7.4 (ALSA-2023:2903)

960657 Rocky Linux Security Update for php:8.0 (RLSA-2023:0848)

960904 Rocky Linux Security Update for Hypertext Preprocessor (PHP) (RLSA-2023:0965)