Tesorion Vulnerability Explorer

Powered by EPSS

Roel van der Jagt | Tesorion

Classification: Public

TESORION

Certifications & partnerships

bsi. ISO/IEC 27001 Information Security Management | NEN 7510 Information Security in Healthcare

EUROPOL The No More Ransom Project | EC3 European Cybercrime Centre

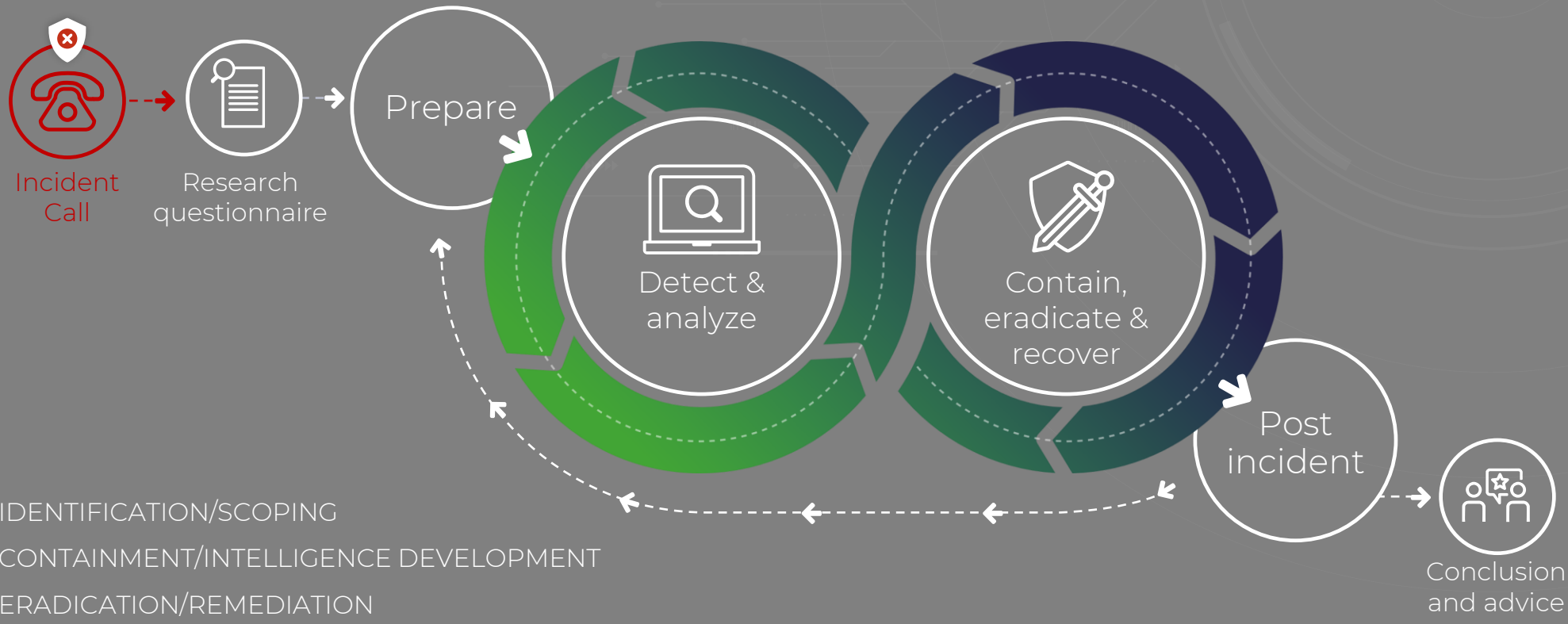
PERSONAL INTRODUCTION

Scroll down

ROEL VAN DER JAGT

T-CERT

INCIDENT RESPONSE APPROACH



- IDENTIFICATION/SCOPING
- CONTAINMENT/INTELLIGENCE DEVELOPMENT
- ERADICATION/REMEDIATION
- AVOIDING "**WHACK-A-MOLE**" INCIDENT RESPONSE

TVE

BACKGROUND

" It is not always **Colonel Mustard** in the **remote access VPN solution** with the **leaked user credentials**."

" The Adversary trail may lead to something, which magically led to initial access, privilege escalation or lateral movement."

" Quick identification of relevant vulnerabilities enhances the abilities of Incident Response teams to minimise impact."

TVE

"Tesorion Vulnerability Explorer is built to help **Incident Response teams** identify software **vulnerabilities** in applications, **prioritized by likelihood** of exploitation. This is done by combining information from six scoring systems and frameworks."


Username : admin
Password : admin

OLDER VULNERABILITIES

Tesorion Vulnerability Explorer

CPE filter: cpe:2.3:*:citrix:netscaler* Filter on CPE NVD CPE search (open website)

CVE filter (comma separated): Filter on CVE

File filter path: TXT Filter on File Clear filter Active filter: CPE

CVE	CVE Published	CVE Last modified	CVSS Ba	CVSS Ve	EPSS Score	EPSS Percentil	EPSS Date	CISA KEV Date	Description
CVE-2019-19781	2019-12-27T14:15Z	2023-01-20T16:21Z	9.8	V3	0.97541	0.9999	2023-09-10	2021-11-03	An issue was discovered in Citrix Application Delivery Controller (ADC) and Gateway 10.5, 11.1, 12.0, 12.1, and 13.(
CVE-2020-8193	2020-07-10T16:15Z	2022-09-20T17:52Z	6.5	V3	0.97454	0.99925	2023-09-10	2021-11-03	Improper access control in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-6
CVE-2019-12985	2019-07-16T18:15Z	2020-08-24T17:37Z	9.8	V3	0.97433	0.99904	2023-09-10	None	Citrix SD-WAN 10.2.x before 10.2.3 and NetScaler SD-WAN 10.0.x before 10.0.8 have Improper Input Validation (iss
CVE-2019-12986	2019-07-16T18:15Z	2020-08-24T17:37Z	9.8	V3	0.97433	0.99904	2023-09-10	None	Citrix SD-WAN 10.2.x before 10.2.3 and NetScaler SD-WAN 10.0.x before 10.0.8 have Improper Input Validation (iss
CVE-2019-12987	2019-07-16T18:15Z	2020-08-24T17:37Z	9.8	V3	0.97433	0.99904	2023-09-10	None	Citrix SD-WAN 10.2.x before 10.2.3 and NetScaler SD-WAN 10.0.x before 10.0.8 have Improper Input Validation (iss
CVE-2019-12988	2019-07-16T18:15Z	2020-08-24T17:37Z	9.8	V3	0.97433	0.99904	2023-09-10	None	Citrix SD-WAN 10.2.x before 10.2.3 and NetScaler SD-WAN 10.0.x before 10.0.8 have Improper Input Validation (iss
CVE-2020-8194	2020-07-10T16:15Z	2020-07-13T20:51Z	6.5	V3	0.97341	0.99825	2023-09-10	None	Reflected code injection in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-6
CVE-2017-6316	2017-07-20T04:29Z	2017-09-16T01:29Z	9.8	V3	0.96168	0.99297	2023-09-10	2022-03-25	Citrix NetScaler SD-WAN devices through v9.1.2.26.561201 allow remote attackers to execute arbitrary shell comr
CVE-2019-12990	2019-07-16T18:15Z	2019-07-17T13:31Z	9.8	V3	0.95724	0.99179	2023-09-10	None	Citrix SD-WAN 10.2.x before 10.2.3 and NetScaler SD-WAN 10.0.x before 10.0.8 allow Directory Traversal.
CVE-2019-12992	2019-07-16T18:15Z	2020-08-24T17:37Z	8.8	V3	0.93837	0.98807	2023-09-10	None	Citrix SD-WAN 10.2.x before 10.2.3 and NetScaler SD-WAN 10.0.x before 10.0.8 have Improper Input Validation (iss
CVE-2023-3519	2023-07-19T18:15Z	2023-08-04T18:15Z	9.8	V3	0.91199	0.98494	2023-09-10	2023-07-19	Unauthenticated remote code execution
CVE-2019-10883	2019-06-03T21:29Z	2020-08-24T17:37Z	9.8	V3	0.88951	0.98307	2023-09-10	None	Citrix SD-WAN Center 10.2.x before 10.2.1 and NetScaler SD-WAN Center 10.0.x before 10.0.7 allow Command Inj
CVE-2020-8195	2020-07-10T16:15Z	2022-09-20T17:23Z	6.5	V3	0.86942	0.98189	2023-09-10	2021-11-03	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-
CVE-2014-7140	2014-10-21T14:55Z	2015-11-25T20:35Z	7.5	V2	0.41183	0.96824	2023-09-10	None	Unspecified vulnerability in the management interface in Citrix NetScaler Application Delivery Controller (ADC) ar
CVE-2019-12991	2019-07-16T18:15Z	2020-08-24T17:37Z	8.8	V3	0.12426	0.94723	2023-09-10	2022-03-25	Citrix SD-WAN 10.2.x before 10.2.3 and NetScaler SD-WAN 10.0.x before 10.0.8 have Improper Input Validation (iss
CVE-2015-2841	2015-04-03T14:59Z	2016-12-03T03:06Z	5.0	V2	0.07283	0.93224	2023-09-10	None	Citrix NetScaler AppFirewall, as used in NetScaler 10.5, allows remote attackers to bypass intended firewall restrict
CVE-2019-12989	2019-07-16T18:15Z	2020-03-30T15:34Z	9.8	V3	0.05976	0.92535	2023-09-10	2022-03-25	Citrix SD-WAN 10.2.x before 10.2.3 and NetScaler SD-WAN 10.0.x before 10.0.8 allow SQL Injection.
CVE-2018-7218	2018-05-17T19:29Z	2018-06-27T18:45Z	9.8	V3	0.01938	0.87203	2023-09-10	None	The AppFirewall functionality in Citrix NetScaler Application Delivery Controller and NetScaler Gateway 10.5 befor
CVE-2015-2838	2015-04-03T14:59Z	2018-10-09T19:56Z	6.8	V2	0.00622	0.76272	2023-09-10	None	Cross-site request forgery (CSRF) vulnerability in Nitro API in Citrix NetScaler before 10.5 build 52.3nc allows remc

TIME TO DO SOME COOKING

INGREDIENTS

- **CVE** Used to identify vulnerabilities.
- **CVSS** The potential impact of a vulnerability.
- **EPSS** The likelihood a vulnerability will be exploited.
- **CPE** Filter vulnerabilities for a specific product.
- **CISA KEV** Reference for known exploited vulnerabilities.
- **CWE** Most common software and hardware weakness types.
- **OSV** An open approach for vulnerability information for open source.

EPSS

"A system to score the likelihood a vulnerability will be exploited in the next 30 days for a given date."

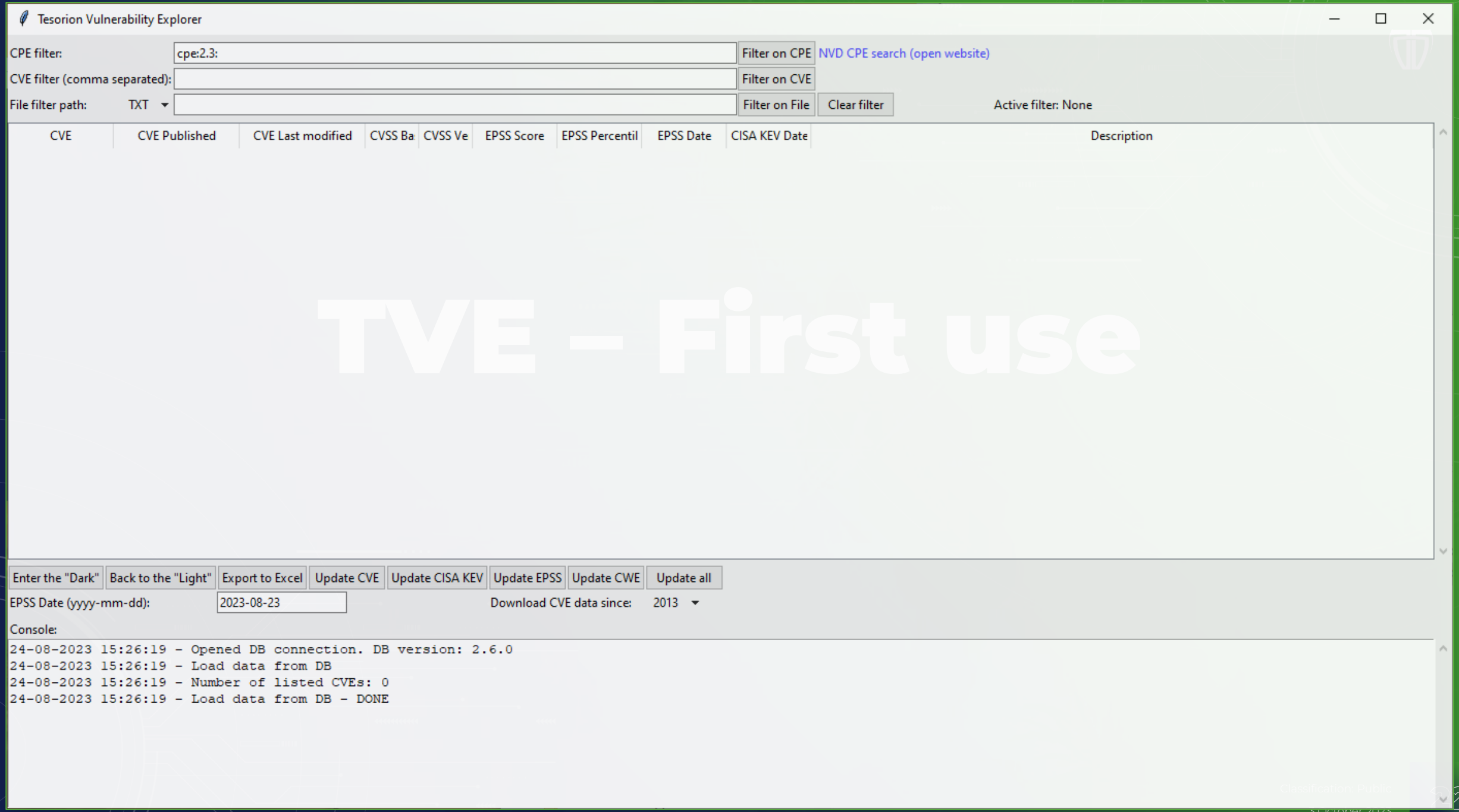
- **EPSS Score** Represents the probability [0-1] of exploitation in the wild in the next 30 days.
- **EPSS Percentile** Proportion of all scored vulnerabilities with the same or a lower EPSS score.

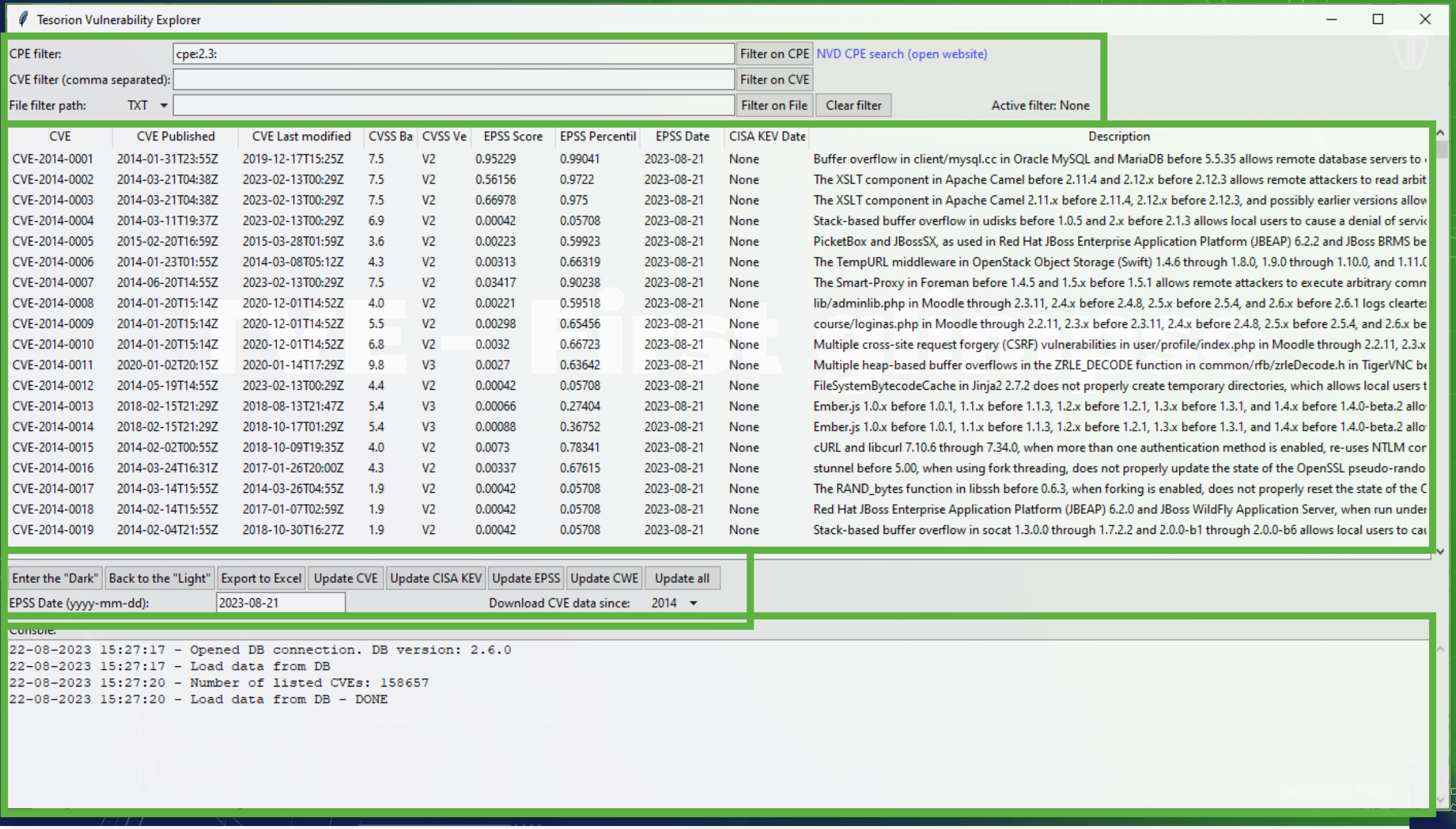
EPSS

SOURCES

Description	Sources
Exploitation activity in the wild	Fortinet, AlienVault, Shadowserver, GreyNoise
Publicly available exploit code	Exploit-DB, GitHub, MetaSploit
CVE mentioned on list or website	CISA KEV, Google Project Zero, Trend Micro ZDI
Social media	Mentions/discussion on Twitter
Offensive security tools and scanners	Intrigue, sn1per, jaeles, nuclei
References with labels	MITRE CVE List, NVD
Keyword description of vulnerability	Text description in MITRE CVE List
CVSS metrics & CWE	National Vulnerability Database (NVD)
Vendor labels	National Vulnerability Database (NVD)
Age of the vulnerability	Days since CVE published in MITRE CVE list

DEMO TIME


Tesorion Vulnerability Explorer
CPE filter:
cpe:2.3:
Filter on CPE
NVD CPE search (open website)
CVE filter (comma separated):
Filter on CVE
File filter path:
TXT
Filter on File
Clear filter
Active filter: None
CVE
CVE Published
CVE Last modified
CVSS Ba
CVSS Ve
EPSS Score
EPSS Percentil
EPSS Date
CISA KEV Date
Description
TVE - First use
Enter the "Dark"
Back to the "Light"
Export to Excel
Update CVE
Update CISA KEV
Update EPSS
Update CWE
Update all
EPSS Date (yyyy-mm-dd):
2023-08-23
Download CVE data since:
2013
Console:
24-08-2023 15:26:19 - Opened DB connection. DB version: 2.6.0
24-08-2023 15:26:19 - Load data from DB
24-08-2023 15:26:19 - Number of listed CVEs: 0
24-08-2023 15:26:19 - Load data from DB - DONE


Tesorion Vulnerability Explorer
CPE filter:
cpe:2.3:
Filter on CPE
NVD CPE search (open website)
CVE filter (comma separated):
Filter on CVE
File filter path:
TXT
Filter on File
Clear filter
Active filter: None
CVE CVE Published CVE Last modified CVSS Ba CVSS Ve EPSS Score EPSS Percentil EPSS Date CISA KEV Date Description
CVE-2014-0001 2014-01-31T23:55Z 2019-12-17T15:25Z 7.5 V2 0.95229 0.99041 2023-08-21 None Buffer overflow in client/mysql.cc in Oracle MySQL and MariaDB before 5.5.35 allows remote database servers to
CVE-2014-0002 2014-03-21T04:38Z 2023-02-13T00:29Z 7.5 V2 0.56156 0.9722 2023-08-21 None The XSLT component in Apache Camel before 2.11.4 and 2.12.x before 2.12.3 allows remote attackers to read arbit
CVE-2014-0003 2014-03-21T04:38Z 2023-02-13T00:29Z 7.5 V2 0.66978 0.975 2023-08-21 None The XSLT component in Apache Camel 2.11.x before 2.11.4, 2.12.x before 2.12.3, and possibly earlier versions allow
CVE-2014-0004 2014-03-11T19:37Z 2023-02-13T00:29Z 6.9 V2 0.00042 0.05708 2023-08-21 None Stack-based buffer overflow in udisks before 1.0.5 and 2.x before 2.1.3 allows local users to cause a denial of servi
CVE-2014-0005 2015-02-20T16:59Z 2015-03-28T01:59Z 3.6 V2 0.00223 0.59923 2023-08-21 None PicketBox and JBossSX, as used in Red Hat JBoss Enterprise Application Platform (JBEAP) 6.2.2 and JBoss BRMS be
CVE-2014-0006 2014-01-23T01:55Z 2014-03-08T05:12Z 4.3 V2 0.00313 0.66319 2023-08-21 None The TempURL middleware in OpenStack Object Storage (Swift) 1.4.6 through 1.8.0, 1.9.0 through 1.10.0, and 1.11.
CVE-2014-0007 2014-06-20T14:55Z 2023-02-13T00:29Z 7.5 V2 0.03417 0.90238 2023-08-21 None The Smart-Proxy in Foreman before 1.4.5 and 1.5.x before 1.5.1 allows remote attackers to execute arbitrary comm
CVE-2014-0008 2014-01-20T15:14Z 2020-12-01T14:52Z 4.0 V2 0.00221 0.59518 2023-08-21 None lib/adminlib.php in Moodle through 2.3.11, 2.4.x before 2.4.8, 2.5.x before 2.5.4, and 2.6.x before 2.6.1 logs cleare
CVE-2014-0009 2014-01-20T15:14Z 2020-12-01T14:52Z 5.5 V2 0.00298 0.65456 2023-08-21 None course/loginas.php in Moodle through 2.2.11, 2.3.x before 2.3.11, 2.4.x before 2.4.8, 2.5.x before 2.5.4, and 2.6.x be
CVE-2014-0010 2014-01-20T15:14Z 2020-12-01T14:52Z 6.8 V2 0.0032 0.66723 2023-08-21 None Multiple cross-site request forgery (CSRF) vulnerabilities in user/profile/index.php in Moodle through 2.2.11, 2.3.x
CVE-2014-0011 2020-01-02T20:15Z 2020-01-14T17:29Z 9.8 V3 0.0027 0.63642 2023-08-21 None Multiple heap-based buffer overflows in the ZRLE_DECODE function in common/rfb/zrleDecode.h in TigerVNC be
CVE-2014-0012 2014-05-19T14:55Z 2023-02-13T00:29Z 4.4 V2 0.00042 0.05708 2023-08-21 None FileSystemBytecodeCache in Jinja2 2.7.2 does not properly create temporary directories, which allows local users t
CVE-2014-0013 2018-02-15T21:29Z 2018-08-13T21:47Z 5.4 V3 0.00066 0.27404 2023-08-21 None Ember.js 1.0.x before 1.0.1, 1.1.x before 1.1.3, 1.2.x before 1.2.1, 1.3.x before 1.3.1, and 1.4.x before 1.4.0-beta.2 allo
CVE-2014-0014 2018-02-15T21:29Z 2018-10-17T01:29Z 5.4 V3 0.00088 0.36752 2023-08-21 None Ember.js 1.0.x before 1.0.1, 1.1.x before 1.1.3, 1.2.x before 1.2.1, 1.3.x before 1.3.1, and 1.4.x before 1.4.0-beta.2 allo
CVE-2014-0015 2014-02-02T00:55Z 2018-10-09T19:35Z 4.0 V2 0.0073 0.78341 2023-08-21 None cURL and libcurl 7.10.6 through 7.34.0, when more than one authentication method is enabled, re-uses NTLM cor
CVE-2014-0016 2014-03-24T16:31Z 2017-01-26T20:00Z 4.3 V2 0.00337 0.67615 2023-08-21 None stunnel before 5.00, when using fork threading, does not properly update the state of the OpenSSL pseudo-rando
CVE-2014-0017 2014-03-14T15:55Z 2014-03-26T04:55Z 1.9 V2 0.00042 0.05708 2023-08-21 None The RAND_bytes function in libssh before 0.6.3, when forking is enabled, does not properly reset the state of the C
CVE-2014-0018 2014-02-14T15:55Z 2017-01-07T02:59Z 1.9 V2 0.00042 0.05708 2023-08-21 None Red Hat JBoss Enterprise Application Platform (JBEAP) 6.2.0 and JBoss WildFly Application Server, when run under
CVE-2014-0019 2014-02-04T21:55Z 2018-10-30T16:27Z 1.9 V2 0.00042 0.05708 2023-08-21 None Stack-based buffer overflow in socat 1.3.0.0 through 1.7.2.2 and 2.0.0-b1 through 2.0.0-b6 allows local users to ca
Enter the "Dark"
Back to the "Light"
Export to Excel
Update CVE
Update CISA KEV
Update EPSS
Update CWE
Update all
EPSS Date (yyyy-mm-dd):
2023-08-21
Download CVE data since:
2014
Console:
22-08-2023 15:27:17 - Opened DB connection. DB version: 2.6.0
22-08-2023 15:27:17 - Load data from DB
22-08-2023 15:27:20 - Number of listed CVEs: 158657
22-08-2023 15:27:20 - Load data from DB - DONE

Tesorion Vulnerability Explorer

CPE filter: cpe:2.3:*:citrix:netscaler* | Filter on CPE | NVD CPE search (open website)

CVE filter (comma separated): | Filter on CVE

File filter path: TXT | Filter on File | Clear filter | Active filter: CPE

CVE	CVE Published	CVE Last modified	CVSS Ba	CVSS Ve	EPSS Score	EPSS Percentil	EPSS Date	CISA KEV Date	Description
CVE-2023-3519	2023-07-19T18:15Z	2023-08-04T18:15Z	9.8	V3	0.91199	0.98471	2023-08-21	2023-07-19	Unauthenticated remote code execution
CVE-2023-3467	2023-07-19T19:15Z	2023-07-28T14:54Z	8.0	V3	0.00043	0.06991	2023-08-21	None	Privilege Escalation to root administrator (nsroot)
CVE-2023-3466	2023-07-19T19:15Z	2023-07-28T14:54Z	6.1	V3	0.00046	0.13991	2023-08-21	None	Reflected Cross-Site Scripting (XSS)
CVE-2021-22927	2021-08-05T21:15Z	2021-08-16T20:14Z	8.1	V3	0.00152	0.50812	2023-08-21	None	A session fixation vulnerability exists in Citrix ADC and Citrix Gateway 13.0-82.45 when configured SAML service p
CVE-2021-22919	2021-08-05T21:15Z	2021-08-16T16:54Z	7.5	V3	0.00089	0.3719	2023-08-21	None	A vulnerability has been discovered in Citrix ADC (formerly known as NetScaler ADC) and Citrix Gateway (formerl
CVE-2020-8300	2021-06-16T14:15Z	2022-09-20T17:23Z	6.5	V3	0.00073	0.30367	2023-08-21	None	Citrix ADC and Citrix/NetScaler Gateway before 13.0-82.41, 12.1-62.23, 11.1-65.20 and Citrix ADC 12.1-FIPS before
CVE-2020-8299	2021-06-16T14:15Z	2021-06-24T20:23Z	6.5	V3	0.0005	0.17262	2023-08-21	None	Citrix ADC and Citrix/NetScaler Gateway 13.0 before 13.0-76.29, 12.1-61.18, 11.1-65.20, Citrix ADC 12.1-FIPS before
CVE-2020-8247	2020-09-18T21:15Z	2020-10-07T15:45Z	8.8	V3	0.00104	0.41776	2023-08-21	None	Citrix ADC and Citrix Gateway 13.0 before 13.0-64.35, Citrix ADC and NetScaler Gateway 12.1 before 12.1-58.15, Cit
CVE-2020-8246	2020-09-18T21:15Z	2020-10-07T15:43Z	7.5	V3	0.00103	0.41521	2023-08-21	None	Citrix ADC and Citrix Gateway 13.0 before 13.0-64.35, Citrix ADC and NetScaler Gateway 12.1 before 12.1-58.15, Cit
CVE-2020-8245	2020-09-18T21:15Z	2020-10-07T16:18Z	6.1	V3	0.00078	0.32485	2023-08-21	None	Improper Input Validation on Citrix ADC and Citrix Gateway 13.0 before 13.0-64.35, Citrix ADC and NetScaler Gate
CVE-2020-8198	2020-07-10T16:15Z	2020-07-13T20:41Z	6.1	V3	0.00078	0.32485	2023-08-21	None	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-
CVE-2020-8197	2020-07-10T16:15Z	2021-07-21T11:39Z	8.8	V3	0.00102	0.4098	2023-08-21	None	Privilege escalation vulnerability on Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.2
CVE-2020-8196	2020-07-10T16:15Z	2022-09-20T17:23Z	4.3	V3	0.00201	0.57223	2023-08-21	2021-11-03	Improper access control in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-6
CVE-2020-8195	2020-07-10T16:15Z	2022-09-20T17:23Z	6.5	V3	0.86942	0.98171	2023-08-21	2021-11-03	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-
CVE-2020-8194	2020-07-10T16:15Z	2020-07-13T20:51Z	6.5	V3	0.97341	0.99823	2023-08-21	None	Reflected code injection in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-6
CVE-2020-8193	2020-07-10T16:15Z	2022-09-20T17:52Z	6.5	V3	0.97454	0.99924	2023-08-21	2021-11-03	Improper access control in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-6
CVE-2020-8191	2020-07-10T16:15Z	2020-07-13T20:40Z	6.1	V3	0.0021	0.58191	2023-08-21	None	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-
CVE-2020-8190	2020-07-10T16:15Z	2020-07-13T20:51Z	7.5	V3	0.00104	0.41776	2023-08-21	None	Incorrect file permissions in Citrix ADC and Citrix Gateway before versions 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-
CVE-2020-8187	2020-07-10T16:15Z	2020-07-13T20:57Z	7.5	V3	0.0011	0.43477	2023-08-21	None	Improper input validation in Citrix ADC and Citrix Gateway versions before 11.1-63.9 and 12.0-62.10 allows unauth

Enter the "Dark" | Back to the "Light" | Export to Excel | Update CVE | Update CISA KEV | Update EPSS | Update CWE | Update all

EPSS Date (yyyy-mm-dd): 2023-08-21 | Download CVE data since: 2014

Console:

```
-2013-6941","CVE-2013-6942","CVE-2013-6943","CVE-2013-6944","CVE-2014-7140","CVE-2015-5080","CVE-2015-5538","CVE-2015-6672","CVE-2015-7996","CVE-2015-7997","CVE-2015-7998",
"CVE-2015-2829","CVE-2018-6811","CVE-2014-8580","CVE-2018-18517","CVE-2015-2838","CVE-2015-2839","CVE-2015-2840","CVE-2015-2841","CVE-2017-14602","CVE-2017-17382","CVE-2017
-17549","CVE-2017-7219","CVE-2018-7218","CVE-2019-18225","CVE-2019-19781","CVE-2020-8190","CVE-2020-8191","CVE-2020-8193","CVE-2020-8194","CVE-2020-8195","CVE-2020-8196","C
VE-2020-8197","CVE-2020-8198","CVE-2018-6186","CVE-2017-6316","CVE-2019-11550","CVE-2018-17444","CVE-2018-17445","CVE-2018-17446","CVE-2018-17447","CVE-2018-17448","CVE-201
9-12985","CVE-2019-12986","CVE-2019-12987","CVE-2019-12988","CVE-2019-12989","CVE-2019-12990","CVE-2019-12991","CVE-2019-12992","CVE-2019-10883","CVE-2019-11345","CVE-2020-
6175","CVE-2020-8187","CVE-2020-8245","CVE-2020-8246","CVE-2020-8247","CVE-2016-4945","CVE-2013-3619","CVE-2013-3620","CVE-2018-5314","CVE-2020-8299","CVE-2020-8300","CVE-2
021-22919","CVE-2021-22927","CVE-2023-3466","CVE-2023-3467","CVE-2023-3519"
22-08-2023 13:09:20 - Number of listed CVEs: 76
22-08-2023 13:09:20 - Load data from DB - DONE
```

CPE explained

cpe:2.3:a:citrix:netscaler:*

Element	Description
cpe:2.3	Schema version
a	Part – “a” is the abbreviation of Application, Other options are “o” for operating system and “h” for hardware
citrix	Vendor
netscaler	Product
*	A wildcard is used for the fields: version, update and edition

Tesorion Vulnerability Explorer

CPE filter: cpe:2.3:*:citrix:netscaler* | Filter on CPE | NVD CPE search (open website)

CVE filter (comma separated): | Filter on CVE

File filter path: TXT | Filter on File | Clear filter | Active filter: CPE

CVE	CVE Published	CVE Last modified	CVSS Ba	CVSS Ve	EPSS Score	EPSS Percentil	EPSS Date	CISA KEV Date	Description
CVE-2023-3519	2023-07-19T18:15Z	2023-08-04T18:15Z	9.8	V3	0.91199	0.98471	2023-08-21	2023-07-19	Unauthenticated remote code execution
CVE-2023-3467	2023-07-19T19:15Z	2023-07-28T14:54Z	8.0	V3	0.00043	0.06991	2023-08-21	None	Privilege Escalation to root administrator (nsroot)
CVE-2023-3466	2023-07-19T19:15Z	2023-07-28T14:54Z	6.1	V3	0.00046	0.13991	2023-08-21	None	Reflected Cross-Site Scripting (XSS)
CVE-2021-22927	2021-08-05T21:15Z	2021-08-16T20:14Z	8.1	V3	0.00152	0.50812	2023-08-21	None	A session fixation vulnerability exists in Citrix ADC and Citrix Gateway 13.0-82.45 when configured SAML service p
CVE-2021-22919	2021-08-05T21:15Z	2021-08-16T16:54Z	7.5	V3	0.00089	0.3719	2023-08-21	None	A vulnerability has been discovered in Citrix ADC (formerly known as NetScaler ADC) and Citrix Gateway (formerl
CVE-2020-8300	2021-06-16T14:15Z	2022-09-20T17:23Z	6.5	V3	0.00073	0.30367	2023-08-21	None	Citrix ADC and Citrix/NetScaler Gateway before 13.0-82.41, 12.1-62.23, 11.1-65.20 and Citrix ADC 12.1-FIPS before
CVE-2020-8299	2021-06-16T14:15Z	2021-06-24T20:23Z	6.5	V3	0.0005	0.17262	2023-08-21	None	Citrix ADC and Citrix/NetScaler Gateway 13.0 before 13.0-76.29, 12.1-61.18, 11.1-65.20, Citrix ADC 12.1-FIPS before
CVE-2020-8247	2020-09-18T21:15Z	2020-10-07T15:45Z	8.8	V3	0.00104	0.41776	2023-08-21	None	Citrix ADC and Citrix Gateway 13.0 before 13.0-64.35, Citrix ADC and NetScaler Gateway 12.1 before 12.1-58.15, Cit
CVE-2020-8246	2020-09-18T21:15Z	2020-10-07T15:43Z	7.5	V3	0.00103	0.41521	2023-08-21	None	Citrix ADC and Citrix Gateway 13.0 before 13.0-64.35, Citrix ADC and NetScaler Gateway 12.1 before 12.1-58.15, Cit
CVE-2020-8245	2020-09-18T21:15Z	2020-10-07T16:18Z	6.1	V3	0.00078	0.32485	2023-08-21	None	Improper Input Validation on Citrix ADC and Citrix Gateway 13.0 before 13.0-64.35, Citrix ADC and NetScaler Gate
CVE-2020-8198	2020-07-10T16:15Z	2020-07-13T20:41Z	6.1	V3	0.00078	0.32485	2023-08-21	None	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-
CVE-2020-8197	2020-07-10T16:15Z	2021-07-21T11:39Z	8.8	V3	0.00102	0.4098	2023-08-21	None	Privilege escalation vulnerability on Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.2
CVE-2020-8196	2020-07-10T16:15Z	2022-09-20T17:23Z	4.3	V3	0.00201	0.57223	2023-08-21	2021-11-03	Improper access control in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-6
CVE-2020-8195	2020-07-10T16:15Z	2022-09-20T17:23Z	6.5	V3	0.86942	0.98171	2023-08-21	2021-11-03	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-
CVE-2020-8194	2020-07-10T16:15Z	2020-07-13T20:51Z	6.5	V3	0.97341	0.99823	2023-08-21	None	Reflected code injection in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-6
CVE-2020-8193	2020-07-10T16:15Z	2022-09-20T17:52Z	6.5	V3	0.97454	0.99924	2023-08-21	2021-11-03	Improper access control in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-6
CVE-2020-8191	2020-07-10T16:15Z	2020-07-13T20:40Z	6.1	V3	0.0021	0.58191	2023-08-21	None	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-
CVE-2020-8190	2020-07-10T16:15Z	2020-07-13T20:51Z	7.5	V3	0.00104	0.41776	2023-08-21	None	Incorrect file permissions in Citrix ADC and Citrix Gateway before versions 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-
CVE-2020-8187	2020-07-10T16:15Z	2020-07-13T20:57Z	7.5	V3	0.0011	0.43477	2023-08-21	None	Improper input validation in Citrix ADC and Citrix Gateway versions before 11.1-63.9 and 12.0-62.10 allows unauth

Enter the "Dark" | Back to the "Light" | Export to Excel | Update CVE | Update CISA KEV | Update EPSS | Update CWE | Update all

EPSS Date (yyyy-mm-dd): 2023-08-21 | Download CVE data since: 2014

Console:

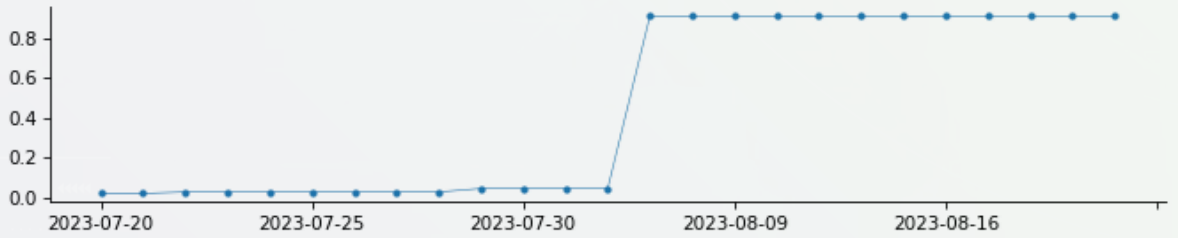
```
-2013-6941","CVE-2013-6942","CVE-2013-6943","CVE-2013-6944","CVE-2014-7140","CVE-2015-5080","CVE-2015-5538","CVE-2015-6672","CVE-2015-7996","CVE-2015-7997","CVE-2015-7998",
"CVE-2015-2829","CVE-2018-6811","CVE-2014-8580","CVE-2018-18517","CVE-2015-2838","CVE-2015-2839","CVE-2015-2840","CVE-2015-2841","CVE-2017-14602","CVE-2017-17382","CVE-2017
-17549","CVE-2017-7219","CVE-2018-7218","CVE-2019-18225","CVE-2019-19781","CVE-2020-8190","CVE-2020-8191","CVE-2020-8193","CVE-2020-8194","CVE-2020-8195","CVE-2020-8196","C
VE-2020-8197","CVE-2020-8198","CVE-2018-6186","CVE-2017-6316","CVE-2019-11550","CVE-2018-17444","CVE-2018-17445","CVE-2018-17446","CVE-2018-17447","CVE-2018-17448","CVE-201
9-12985","CVE-2019-12986","CVE-2019-12987","CVE-2019-12988","CVE-2019-12989","CVE-2019-12990","CVE-2019-12991","CVE-2019-12992","CVE-2019-10883","CVE-2019-11345","CVE-2020-
6175","CVE-2020-8187","CVE-2020-8245","CVE-2020-8246","CVE-2020-8247","CVE-2016-4945","CVE-2013-3619","CVE-2013-3620","CVE-2018-5314","CVE-2020-8299","CVE-2020-8300","CVE-2
021-22919","CVE-2021-22927","CVE-2023-3466","CVE-2023-3467","CVE-2023-3519"
22-08-2023 13:09:20 - Number of listed CVEs: 76
22-08-2023 13:09:20 - Load data from DB - DONE
```

CVE Details - CVE-2023-3519

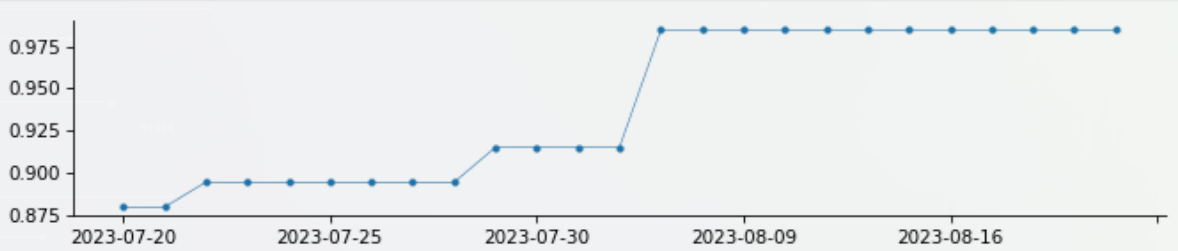
NVD CVE Details (open website)

CVE ID	CVE-2023-3519
CVE Published	2023-07-19T18:15Z
CVE Last modified	2023-08-04T18:15Z
CVSS Base score	9.8
CVSS Version	V3
CVSS VectorString	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CWE ID	CWE-94
CWE Description	Improper Control of Generation of Code ('Code Injection')
EPSS Score	0.91199
EPSS Percentile	0.98471
EPSS Date	2023-08-21
CISA KEV Date	2023-07-19
CVE Description	Unauthenticated remote code execution
CVE References	https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467 http://packetstormsecurity.com/files/173997/Citrix-ADC-NetScaler-Remote-Code-Execution.html

Trendline EPSS Score



Trendline EPSS Percentile



Tesorion Vulnerability Explorer

CPE filter: cpe:2.3: | Filter on CPE | NVD CPE search (open website)

CVE filter (comma separated): CVE-2023-35078,CVE-2023-35081,CVE-2023-35082,CVE-2023-38035,CVE-2023-32560 | Filter on CVE

File filter path: TXT | Filter on File | Clear filter | Active filter: CVE

CVE	CVE Published	CVE Last modified	CVSS Ba	CVSS Ve	EPSS Score	EPSS Percentil	EPSS Date	CISA KEV Date	Description
CVE-2023-38035	2023-08-21T17:15Z	2023-08-21T18:35Z	None	None	None	None	None	None	A security vulnerability in MICS Admin Portal in Ivanti Mobilelron Sentry versions 9.18.0 and below, which may all
CVE-2023-35082	2023-08-15T16:15Z	2023-08-22T02:16Z	9.8	V3	0.00061	0.23896	2023-08-21	None	An authentication bypass vulnerability in Ivanti EPMM 11.10 and older, allows unauthorized users to access restric
CVE-2023-32560	2023-08-10T20:15Z	2023-08-16T13:04Z	9.8	V3	0.00134	0.479	2023-08-21	None	An attacker can send a specially crafted message to the Wavelink Avalanche Manager, which could result in servic
CVE-2023-35081	2023-08-03T18:15Z	2023-08-08T20:25Z	7.2	V3	0.62318	0.97384	2023-08-21	2023-07-31	A path traversal vulnerability in Ivanti EPMM versions (11.10.x < 11.10.0.3, 11.9.x < 11.9.1.2 and 11.8.x < 11.8.1.2) a
CVE-2023-35078	2023-07-25T07:15Z	2023-08-04T18:30Z	9.8	V3	0.96524	0.99411	2023-08-21	2023-07-25	

Enter the "Dark" | Back to the "Light" | Export to Excel | Update CVE | Update CISA KEV | Update EPSS | Update CWE | Update all

EPSS Date (yyyy-mm-dd): 2023-08-21 | Download CVE data since: 2014

Console:

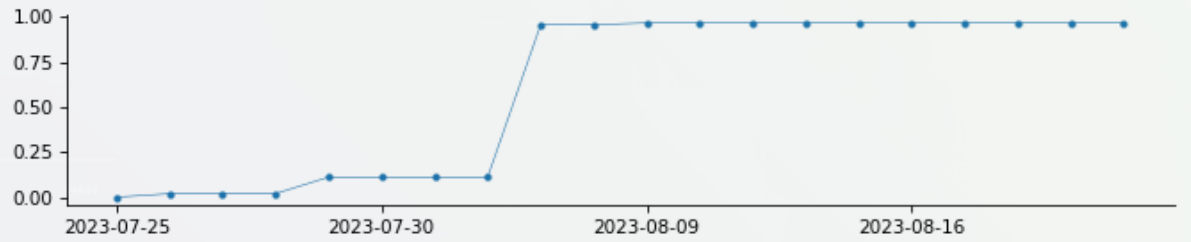
```
22-08-2023 16:01:14 - Load data from DB
22-08-2023 16:01:14 - Filter on CVE(s): "CVE-2023-35078","CVE-2023-35081","CVE-2023-35082","CVE-2023-38035","CVE-2023-32560"
22-08-2023 16:01:14 - Number of listed CVEs: 5
22-08-2023 16:01:14 - Load data from DB - DONE
22-08-2023 16:02:04 - Sort on: cve.published_date DESC
22-08-2023 16:02:04 - Load data from DB
22-08-2023 16:02:04 - Filter on CVE(s): "CVE-2023-35078","CVE-2023-35081","CVE-2023-35082","CVE-2023-38035","CVE-2023-32560"
22-08-2023 16:02:04 - Number of listed CVEs: 5
22-08-2023 16:02:04 - Load data from DB - DONE
```

CVE Details - CVE-2023-35078

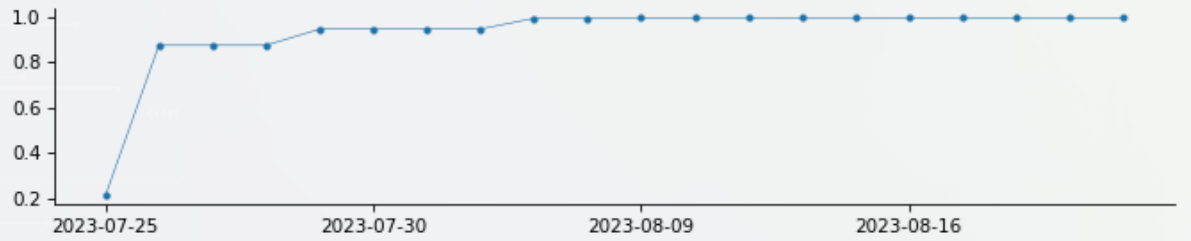
NVD CVE Details (open website)

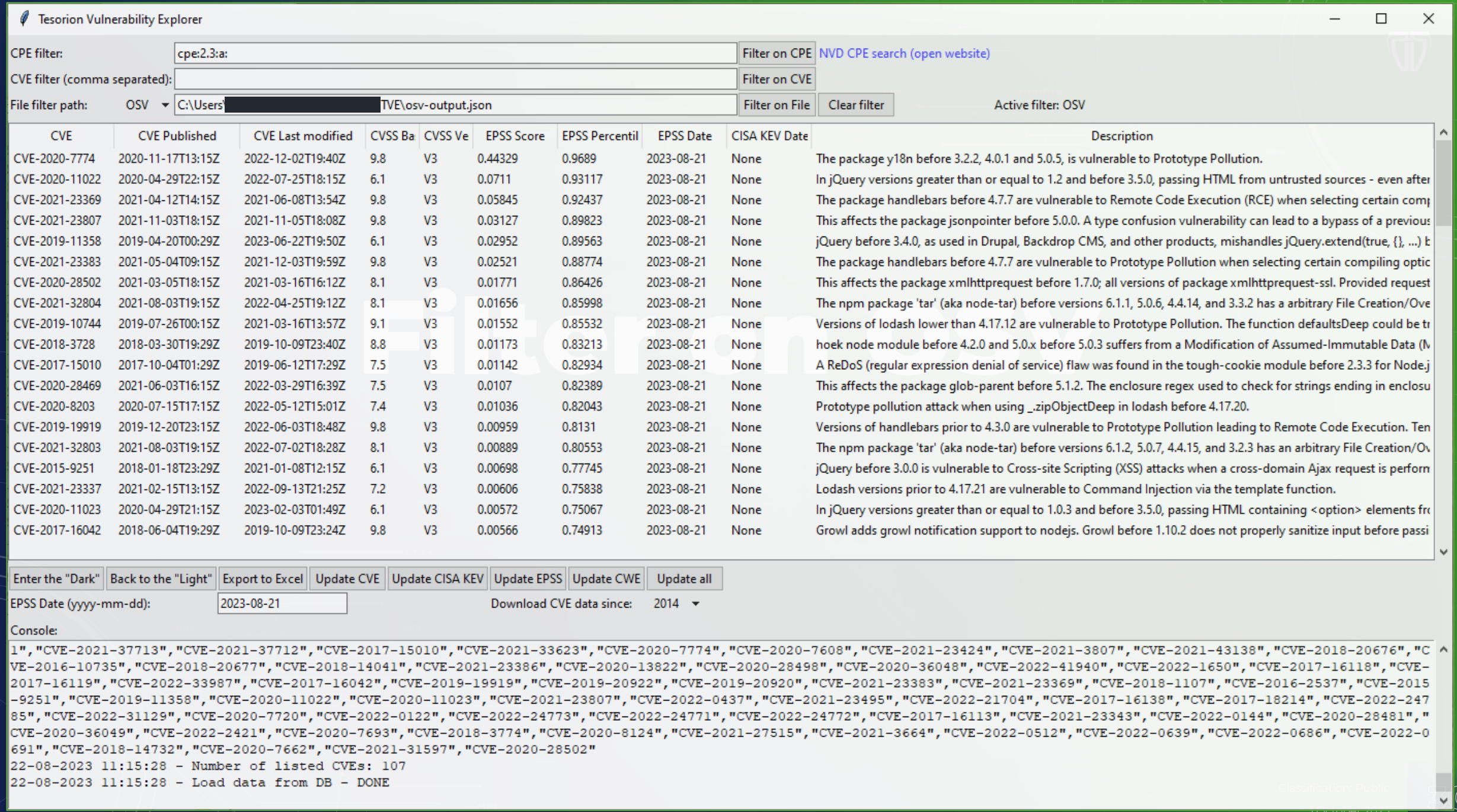
CVE ID	CVE-2023-35078
CVE Published	2023-07-25T07:15Z
CVE Last modified	2023-08-04T18:30Z
CVSS Base score	9.8
CVSS Version	V3
CVSS VectorString	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CWE ID	CWE-287
CWE Description	Improper Authentication
EPSS Score	0.96524
EPSS Percentile	0.99411
EPSS Date	2023-08-21
CISA KEV Date	2023-07-25
CVE Description	Ivanti Endpoint Manager Mobile (EPMM), formerly MobileIron Core, through 11.10 allows remote attackers to obtain PII, add an administrative account, and change the configuration because of an authentication bypass, as exploited in the wild in July 2023. A patch is available.
CVE References	https://www.cisa.gov/news-events/alerts/2023/07/24/ivanti-releases-security-updates-endpoint-manager-mobile-epmm-cve-2023-35078 https://forums.ivanti.com/s/article/CVE-2023-35078-Remote-unauthenticated-API-access-vulnerability https://www.ivanti.com/blog/cve-2023-35078-new-ivanti-epmm-vulnerability

Trendline EPSS Score



Trendline EPSS Percentile




Tesorion Vulnerability Explorer
CPE filter:
cpe:2.3:a:
Filter on CPE
NVD CPE search (open website)
CVE filter (comma separated):
Filter on CVE
File filter path:
OSV
C:\Users[redacted]TVE\osv-output.json
Filter on File
Clear filter
Active filter: OSV
CVE | CVE Published | CVE Last modified | CVSS Ba | CVSS Ve | EPSS Score | EPSS Percentil | EPSS Date | CISA KEV Date | Description
CVE-2020-7774 | 2020-11-17T13:15Z | 2022-12-02T19:40Z | 9.8 | V3 | 0.44329 | 0.9689 | 2023-08-21 | None | The package y18n before 3.2.2, 4.0.1 and 5.0.5, is vulnerable to Prototype Pollution.
CVE-2020-11022 | 2020-04-29T22:15Z | 2022-07-25T18:15Z | 6.1 | V3 | 0.0711 | 0.93117 | 2023-08-21 | None | In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after
CVE-2021-23369 | 2021-04-12T14:15Z | 2021-06-08T13:54Z | 9.8 | V3 | 0.05845 | 0.92437 | 2023-08-21 | None | The package handlebars before 4.7.7 are vulnerable to Remote Code Execution (RCE) when selecting certain comp
CVE-2021-23807 | 2021-11-03T18:15Z | 2021-11-05T18:08Z | 9.8 | V3 | 0.03127 | 0.89823 | 2023-08-21 | None | This affects the package jsonpointer before 5.0.0. A type confusion vulnerability can lead to a bypass of a previous
CVE-2019-11358 | 2019-04-20T00:29Z | 2023-06-22T19:50Z | 6.1 | V3 | 0.02952 | 0.89563 | 2023-08-21 | None | jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) b
CVE-2021-23383 | 2021-05-04T09:15Z | 2021-12-03T19:59Z | 9.8 | V3 | 0.02521 | 0.88774 | 2023-08-21 | None | The package handlebars before 4.7.7 are vulnerable to Prototype Pollution when selecting certain compiling optic
CVE-2020-28502 | 2021-03-05T18:15Z | 2021-03-16T16:12Z | 8.1 | V3 | 0.01771 | 0.86426 | 2023-08-21 | None | This affects the package xmlhttprequest before 1.7.0; all versions of package xmlhttprequest-ssl. Provided request
CVE-2021-32804 | 2021-08-03T19:15Z | 2022-04-25T19:12Z | 8.1 | V3 | 0.01656 | 0.85998 | 2023-08-21 | None | The npm package 'tar' (aka node-tar) before versions 6.1.1, 5.0.6, 4.4.14, and 3.3.2 has a arbitrary File Creation/Ove
CVE-2019-10744 | 2019-07-26T00:15Z | 2021-03-16T13:57Z | 9.1 | V3 | 0.01552 | 0.85532 | 2023-08-21 | None | Versions of lodash lower than 4.17.12 are vulnerable to Prototype Pollution. The function defaultsDeep could be tr
CVE-2018-3728 | 2018-03-30T19:29Z | 2019-10-09T23:40Z | 8.8 | V3 | 0.01173 | 0.83213 | 2023-08-21 | None | hoek node module before 4.2.0 and 5.0.x before 5.0.3 suffers from a Modification of Assumed-Immutable Data (M
CVE-2017-15010 | 2017-10-04T01:29Z | 2019-06-12T17:29Z | 7.5 | V3 | 0.01142 | 0.82934 | 2023-08-21 | None | A ReDoS (regular expression denial of service) flaw was found in the tough-cookie module before 2.3.3 for Node.j
CVE-2020-28469 | 2021-06-03T16:15Z | 2022-03-29T16:39Z | 7.5 | V3 | 0.0107 | 0.82389 | 2023-08-21 | None | This affects the package glob-parent before 5.1.2. The enclosure regex used to check for strings ending in enclosu
CVE-2020-8203 | 2020-07-15T17:15Z | 2022-05-12T15:01Z | 7.4 | V3 | 0.01036 | 0.82043 | 2023-08-21 | None | Prototype pollution attack when using _.zipObjectDeep in lodash before 4.17.20.
CVE-2019-19919 | 2019-12-20T23:15Z | 2022-06-03T18:48Z | 9.8 | V3 | 0.00959 | 0.8131 | 2023-08-21 | None | Versions of handlebars prior to 4.3.0 are vulnerable to Prototype Pollution leading to Remote Code Execution. Ten
CVE-2021-32803 | 2021-08-03T19:15Z | 2022-07-02T18:28Z | 8.1 | V3 | 0.00889 | 0.80553 | 2023-08-21 | None | The npm package 'tar' (aka node-tar) before versions 6.1.2, 5.0.7, 4.4.15, and 3.2.3 has an arbitrary File Creation/Ov
CVE-2015-9251 | 2018-01-18T23:29Z | 2021-01-08T12:15Z | 6.1 | V3 | 0.00698 | 0.77745 | 2023-08-21 | None | jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is perform
CVE-2021-23337 | 2021-02-15T13:15Z | 2022-09-13T21:25Z | 7.2 | V3 | 0.00606 | 0.75838 | 2023-08-21 | None | Lodash versions prior to 4.17.21 are vulnerable to Command Injection via the template function.
CVE-2020-11023 | 2020-04-29T21:15Z | 2023-02-03T01:49Z | 6.1 | V3 | 0.00572 | 0.75067 | 2023-08-21 | None | In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements fr
CVE-2017-16042 | 2018-06-04T19:29Z | 2019-10-09T23:24Z | 9.8 | V3 | 0.00566 | 0.74913 | 2023-08-21 | None | Growl adds growl notification support to nodejs. Growl before 1.10.2 does not properly sanitize input before passi
Enter the "Dark"
Back to the "Light"
Export to Excel
Update CVE
Update CISA KEV
Update EPSS
Update CWE
Update all
EPSS Date (yyyy-mm-dd):
2023-08-21
Download CVE data since:
2014
Console:
1","CVE-2021-37713","CVE-2021-37712","CVE-2017-15010","CVE-2021-33623","CVE-2020-7774","CVE-2020-7608","CVE-2021-23424","CVE-2021-3807","CVE-2021-43138","CVE-2018-20676","C
VE-2016-10735","CVE-2018-20677","CVE-2018-14041","CVE-2021-23386","CVE-2020-13822","CVE-2020-28498","CVE-2020-36048","CVE-2022-41940","CVE-2022-1650","CVE-2017-16118","CVE-
2017-16119","CVE-2022-33987","CVE-2017-16042","CVE-2019-19919","CVE-2019-20922","CVE-2019-20920","CVE-2021-23383","CVE-2021-23369","CVE-2018-1107","CVE-2016-2537","CVE-2015
-9251","CVE-2019-11358","CVE-2020-11022","CVE-2020-11023","CVE-2021-23807","CVE-2022-0437","CVE-2021-23495","CVE-2022-21704","CVE-2017-16138","CVE-2017-18214","CVE-2022-247
85","CVE-2022-31129","CVE-2020-7720","CVE-2022-0122","CVE-2022-24773","CVE-2022-24771","CVE-2022-24772","CVE-2017-16113","CVE-2021-23343","CVE-2022-0144","CVE-2020-28481","
CVE-2020-36049","CVE-2022-2421","CVE-2020-7693","CVE-2018-3774","CVE-2020-8124","CVE-2021-27515","CVE-2021-3664","CVE-2022-0512","CVE-2022-0639","CVE-2022-0686","CVE-2022-0
691","CVE-2018-14732","CVE-2020-7662","CVE-2021-31597","CVE-2020-28502"
22-08-2023 11:15:28 - Number of listed CVEs: 107
22-08-2023 11:15:28 - Load data from DB - DONE

Tesorion Vulnerability Explorer

CPE filter: cpe:2.3: | Filter on CPE | NVD CPE search (open website)

CVE filter (comma separated): | Filter on CVE

File filter path: TXT | C:\Users[redacted]TVE\Sample_data-Oracle_CPU_July_2022_overview.txt | Filter on File | Clear filter | Active filter: TXT

CVE	CVE Published	CVE Last modified	CVSS Ba	CVSS Ve	EPSS Score	EPSS Percentil	EPSS Date	CISA KEV Date	Description
CVE-2022-22947	2022-03-03T22:15Z	2023-07-24T13:47Z	10.0	V3	0.97524	0.99979	2023-08-21	2022-05-16	In spring cloud gateway versions prior to 3.1.1+ and 3.0.7+ , applications are vulnerable to a code injection attack
CVE-2022-22965	2022-04-01T23:15Z	2023-02-09T02:07Z	9.8	V3	0.97523	0.99978	2023-08-21	2022-04-04	A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RC
CVE-2018-1273	2018-04-11T13:29Z	2022-07-25T18:15Z	9.8	V3	0.97498	0.99961	2023-08-21	2022-03-25	Spring Data Commons, versions prior to 1.13 to 1.13.10, 2.0 to 2.0.5, and older unsupported versions, contain a pr
CVE-2019-17571	2019-12-20T17:15Z	2022-12-14T17:50Z	9.8	V3	0.97467	0.99936	2023-08-21	None	Included in Log4j 1.2 is a SocketServer class that is vulnerable to deserialization of untrusted data which can be ex
CVE-2022-22963	2022-04-01T23:15Z	2023-07-13T23:15Z	9.8	V3	0.97452	0.99922	2023-08-21	2022-08-25	In Spring Cloud Function versions 3.1.6, 3.2.2 and older unsupported versions, when using routing functionality it
CVE-2021-39144	2021-08-23T18:15Z	2023-06-26T19:17Z	8.5	V3	0.97244	0.99755	2023-08-21	2023-03-10	XStream is a simple library to serialize objects to XML and back again. In affected versions this vulnerability may a
CVE-2020-5398	2020-01-17T00:15Z	2022-07-25T18:15Z	7.5	V3	0.97208	0.99729	2023-08-21	None	In Spring Framework, versions 5.2.x prior to 5.2.3, versions 5.1.x prior to 5.1.13, and versions 5.0.x prior to 5.0.16, ar
CVE-2020-9484	2020-05-20T19:15Z	2022-07-25T18:15Z	7.0	V3	0.96918	0.9959	2023-08-21	None	When using Apache Tomcat versions 10.0.0-M1 to 10.0.0-M4, 9.0.0.M1 to 9.0.34, 8.5.0 to 8.5.54 and 7.0.0 to 7.0.103
CVE-2019-0227	2019-05-01T21:29Z	2022-07-25T18:15Z	7.5	V3	0.9601	0.99241	2023-08-21	None	A Server Side Request Forgery (SSRF) vulnerability affected the Apache Axis 1.4 distribution that was last released i
CVE-2022-21500	2022-05-20T00:15Z	2022-10-27T16:59Z	7.5	V3	0.95664	0.99151	2023-08-21	None	Vulnerability in Oracle E-Business Suite (component: Manage Proxies). The supported version that is affected is 12
CVE-2021-4104	2021-12-14T12:15Z	2022-10-05T17:53Z	7.5	V3	0.89218	0.98304	2023-08-21	None	JMSAppender in Log4j 1.2 is vulnerable to deserialization of untrusted data when the attacker has write access to t
CVE-2021-34429	2021-07-15T17:15Z	2022-10-27T12:25Z	5.3	V3	0.79921	0.97879	2023-08-21	None	For Eclipse Jetty versions 9.4.37-9.4.42, 10.0.1-10.0.5 & 11.0.1-11.0.5, URIs can be crafted using some encoded char
CVE-2022-1292	2022-05-03T16:15Z	2023-02-14T12:15Z	9.8	V3	0.48893	0.97035	2023-08-21	None	The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is di
CVE-2021-41303	2021-09-17T09:15Z	2022-08-12T17:49Z	9.8	V3	0.33667	0.96499	2023-08-21	None	Apache Shiro before 1.8.0, when using Apache Shiro with Spring Boot, a specially crafted HTTP request may cause
CVE-2021-39141	2021-08-23T18:15Z	2022-10-05T02:35Z	8.5	V3	0.15968	0.9526	2023-08-21	None	XStream is a simple library to serialize objects to XML and back again. In affected versions this vulnerability may a
CVE-2021-39146	2021-08-23T18:15Z	2022-10-05T11:54Z	8.5	V3	0.15366	0.95178	2023-08-21	None	XStream is a simple library to serialize objects to XML and back again. In affected versions this vulnerability may a
CVE-2020-11022	2020-04-29T22:15Z	2022-07-25T18:15Z	6.1	V3	0.0711	0.93117	2023-08-21	None	In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after
CVE-2021-44832	2021-12-28T20:15Z	2022-08-09T01:24Z	6.6	V3	0.0469	0.91605	2023-08-21	None	Apache Log4j2 versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4) are vulnerable to
CVE-2022-29885	2022-05-12T08:15Z	2023-04-06T17:15Z	7.5	V3	0.03165	0.89879	2023-08-21	None	The documentation of Apache Tomcat 10.1.0-M1 to 10.1.0-M14, 10.0.0-M1 to 10.0.20, 9.0.13 to 9.0.62 and 8.5.38 to

Enter the "Dark" | Back to the "Light" | Export to Excel | Update CVE | Update CISA KEV | Update EPSS | Update CWE | Update all

EPSS Date (yyyy-mm-dd): 2023-08-21 | Download CVE data since: 2014

Console:

```
322","CVE-2020-9492","CVE-2020-9484","CVE-2020-7712","CVE-2020-7656","CVE-2020-5398","CVE-2020-5397","CVE-2020-5258","CVE-2020-4788","CVE-2020-36518","CVE-2020-36189","CVE-
2020-36188","CVE-2020-36187","CVE-2020-36186","CVE-2020-36185","CVE-2020-36184","CVE-2020-36183","CVE-2020-36182","CVE-2020-36181","CVE-2020-36180","CVE-2020-36179","CVE-20
20-35728","CVE-2020-35491","CVE-2020-35490","CVE-2020-35169","CVE-2020-35168","CVE-2020-35167","CVE-2020-35166","CVE-2020-35164","CVE-2020-35163","CVE-2020-29651","CVE-2020
-29508","CVE-2020-29507","CVE-2020-29506","CVE-2020-29505","CVE-2020-29396","CVE-2020-28500","CVE-2020-28491","CVE-2020-28052","CVE-2020-27820","CVE-2020-27619","CVE-2020-2
6237","CVE-2020-26185","CVE-2020-26184","CVE-2020-26137","CVE-2020-25649","CVE-2020-1927","CVE-2020-17521","CVE-2020-1747","CVE-2020-14343","CVE-2020-13974","CVE-2020-11987
","CVE-2020-11023","CVE-2020-11022","CVE-2020-10683","CVE-2020-0404","CVE-2019-9740","CVE-2019-9636","CVE-2019-20916","CVE-2019-17571","CVE-2019-17495","CVE-2019-10086","CV
E-2019-10082","CVE-2019-0227","CVE-2019-0220","CVE-2019-0219","CVE-2018-8032","CVE-2018-25032","CVE-2018-18074","CVE-2018-1274","CVE-2018-1273","CVE-2018-1259"
22-08-2023 16:30:45 - Number of listed CVEs: 316
22-08-2023 16:30:45 - Load data from DB - DONE
```

Tesorion Vulnerability Explorer

CPE filter: cpe:2.3: | Filter on CPE | NVD CPE search (open website)

CVE filter (comma separated): | Filter on CVE

File filter path: TXT | C:\Users[redacted]TVE\uniqQvuln.csv | Filter on File | Clear filter | Active filter: TXT

CVE	CVE Published	CVE Last modified	CVSS Ba	CVSS Ve	EPSS Score	EPSS Percentil	EPSS Date	CISA KEV Date	Description
CVE-2017-5753	2018-01-04T13:29Z	2021-11-23T22:14Z	5.6	V3	0.97573	0.99998	2023-08-21	None	Systems with microprocessors utilizing speculative execution and branch prediction may allow unauthorized disc
CVE-2017-5715	2018-01-04T13:29Z	2021-08-16T09:15Z	5.6	V3	0.97549	0.99993	2023-08-21	None	Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthori
CVE-2017-5754	2018-01-04T13:29Z	2021-11-19T18:15Z	5.6	V3	0.97489	0.99954	2023-08-21	None	Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthori
CVE-2018-16509	2018-09-05T06:29Z	2019-10-03T00:03Z	7.8	V3	0.97438	0.99909	2023-08-21	None	An issue was discovered in Artifex Ghostscript before 9.24. Incorrect 'restoration of privilege' checking during han
CVE-2023-21823	2023-02-14T21:15Z	2023-02-23T21:46Z	7.8	V3	0.77882	0.97813	2023-08-21	2023-02-14	Windows Graphics Component Remote Code Execution Vulnerability
CVE-2022-41128	2022-11-09T22:15Z	2023-08-08T14:21Z	8.8	V3	0.55549	0.97206	2023-08-21	2022-11-08	Windows Scripting Languages Remote Code Execution Vulnerability
CVE-2023-21716	2023-02-14T20:15Z	2023-02-23T15:43Z	9.8	V3	0.53469	0.9716	2023-08-21	None	Microsoft Word Remote Code Execution Vulnerability
CVE-2023-21689	2023-02-14T20:15Z	2023-02-24T13:56Z	9.8	V3	0.51309	0.97106	2023-08-21	None	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability
CVE-2023-21690	2023-02-14T20:15Z	2023-02-24T14:04Z	9.8	V3	0.51309	0.97106	2023-08-21	None	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability
CVE-2023-21692	2023-02-14T20:15Z	2023-02-24T15:02Z	9.8	V3	0.51309	0.97106	2023-08-21	None	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability
CVE-2023-21707	2023-02-14T20:15Z	2023-02-23T16:03Z	8.8	V3	0.38084	0.96717	2023-08-21	None	Microsoft Exchange Server Remote Code Execution Vulnerability
CVE-2020-17106	2020-11-11T07:15Z	2020-11-19T21:04Z	7.8	V3	0.1522	0.95147	2023-08-21	None	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2020-17107, CVE-20
CVE-2020-17107	2020-11-11T07:15Z	2020-11-19T20:57Z	7.8	V3	0.1522	0.95147	2023-08-21	None	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2020-17106, CVE-20
CVE-2020-17108	2020-11-11T07:15Z	2020-11-19T20:52Z	7.8	V3	0.1522	0.95147	2023-08-21	None	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2020-17106, CVE-20
CVE-2020-17109	2020-11-11T07:15Z	2020-11-19T20:50Z	7.8	V3	0.1522	0.95147	2023-08-21	None	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2020-17106, CVE-20
CVE-2020-17110	2020-11-11T07:15Z	2020-11-19T20:40Z	7.8	V3	0.1522	0.95147	2023-08-21	None	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2020-17106, CVE-20
CVE-2023-21752	2023-01-10T22:15Z	2023-04-27T19:15Z	7.1	V3	0.13953	0.94958	2023-08-21	None	Windows Backup Service Elevation of Privilege Vulnerability
CVE-2022-38031	2022-10-11T19:15Z	2022-10-12T17:11Z	8.8	V3	0.06315	0.92707	2023-08-21	None	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability. This CVE ID is unique fron
CVE-2022-38040	2022-10-11T19:15Z	2022-10-12T17:16Z	8.8	V3	0.06315	0.92707	2023-08-21	None	Microsoft ODBC Driver Remote Code Execution Vulnerability.

Enter the "Dark" | Back to the "Light" | Export to Excel | Update CVE | Update CISA KEV | Update EPSS | Update CWE | Update all

EPSS Date (yyyy-mm-dd): 2023-08-21 | Download CVE data since: 2014

Console:

```
2023-21697","CVE-2023-21699","CVE-2023-21700","CVE-2023-21701","CVE-2023-21702","CVE-2023-21706","CVE-2023-21707","CVE-2023-21710","CVE-2023-21714","CVE-2023-21715","CVE-20
23-21716","CVE-2023-21721","CVE-2023-21722","CVE-2023-21724","CVE-2023-21725","CVE-2023-21726","CVE-2023-21728","CVE-2023-21730","CVE-2023-21732","CVE-2023-21733","CVE-2023
-21739","CVE-2023-21746","CVE-2023-21747","CVE-2023-21748","CVE-2023-21749","CVE-2023-21750","CVE-2023-21752","CVE-2023-21753","CVE-2023-21754","CVE-2023-21755","CVE-2023-2
1757","CVE-2023-21758","CVE-2023-21759","CVE-2023-21760","CVE-2023-21765","CVE-2023-21766","CVE-2023-21767","CVE-2023-21768","CVE-2023-21771","CVE-2023-21772","CVE-2023-217
73","CVE-2023-21774","CVE-2023-21776","CVE-2023-21794","CVE-2023-21797","CVE-2023-21798","CVE-2023-21799","CVE-2023-21801","CVE-2023-21802","CVE-2023-21803","CVE-2023-21804
","CVE-2023-21805","CVE-2023-21808","CVE-2023-21811","CVE-2023-21812","CVE-2023-21813","CVE-2023-21816","CVE-2023-21817","CVE-2023-21818","CVE-2023-21819","CVE-2023-21820",
"CVE-2023-21822","CVE-2023-21823","CVE-2023-23376"
22-08-2023 16:33:05 - Number of listed CVEs: 335
22-08-2023 16:33:05 - Load data from DB - DONE
```

WARSTORY

Incoming call...

WARSTORY

BLUFF FOR MONEY

WARSTORY

BLUFF FOR MONEY

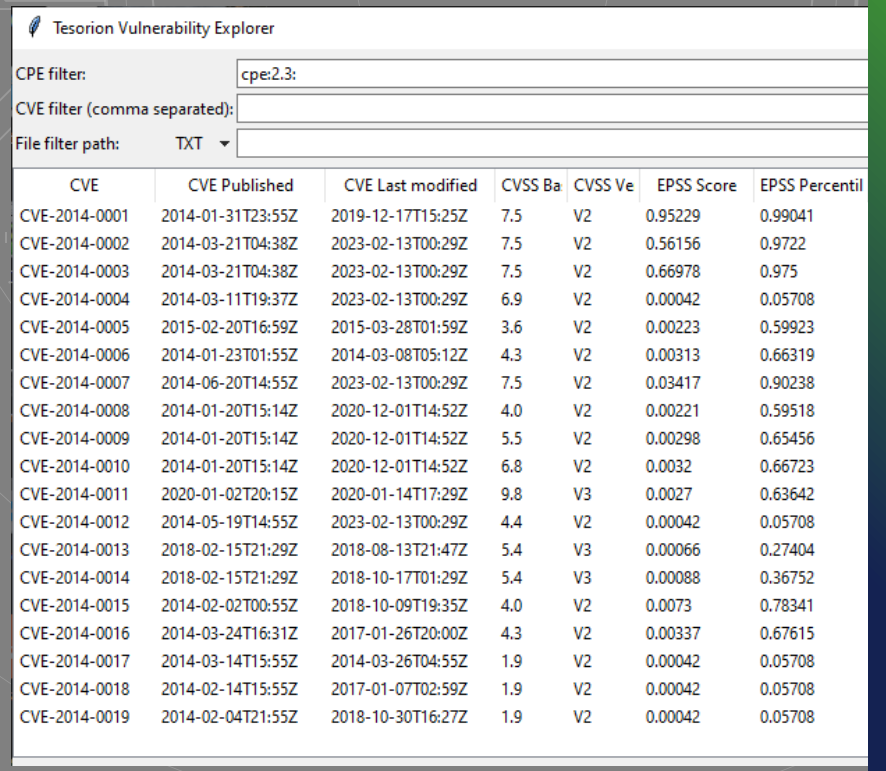
What's next?

Feature roadmap

- Apply multiple CPE filters
- Import CPE from Shodan / Censys export
- Use of CPE API key
- Enrich with Actors (via CWE?)
- EPSS year trend
- Explanation of EPSS score changes

Try it yourself!

GitHub project
https://github.com/tesorion/TCERT-Tesorion_Vulnerability_Explorer



CVE	CVE Published	CVE Last modified	CVSS Ba	CVSS Ve	EPSS Score	EPSS Percentil
CVE-2014-0001	2014-01-31T23:55Z	2019-12-17T15:25Z	7.5	V2	0.95229	0.99041
CVE-2014-0002	2014-03-21T04:38Z	2023-02-13T00:29Z	7.5	V2	0.56156	0.9722
CVE-2014-0003	2014-03-21T04:38Z	2023-02-13T00:29Z	7.5	V2	0.66978	0.975
CVE-2014-0004	2014-03-11T19:37Z	2023-02-13T00:29Z	6.9	V2	0.00042	0.05708
CVE-2014-0005	2015-02-20T16:59Z	2015-03-28T01:59Z	3.6	V2	0.00223	0.59923
CVE-2014-0006	2014-01-23T01:55Z	2014-03-08T05:12Z	4.3	V2	0.00313	0.66319
CVE-2014-0007	2014-06-20T14:55Z	2023-02-13T00:29Z	7.5	V2	0.03417	0.90238
CVE-2014-0008	2014-01-20T15:14Z	2020-12-01T14:52Z	4.0	V2	0.00221	0.59518
CVE-2014-0009	2014-01-20T15:14Z	2020-12-01T14:52Z	5.5	V2	0.00298	0.65456
CVE-2014-0010	2014-01-20T15:14Z	2020-12-01T14:52Z	6.8	V2	0.0032	0.66723
CVE-2014-0011	2020-01-02T20:15Z	2020-01-14T17:29Z	9.8	V3	0.0027	0.63642
CVE-2014-0012	2014-05-19T14:55Z	2023-02-13T00:29Z	4.4	V2	0.00042	0.05708
CVE-2014-0013	2018-02-15T21:29Z	2018-08-13T21:47Z	5.4	V3	0.00066	0.27404
CVE-2014-0014	2018-02-15T21:29Z	2018-10-17T01:29Z	5.4	V3	0.00088	0.36752
CVE-2014-0015	2014-02-02T00:55Z	2018-10-09T19:35Z	4.0	V2	0.0073	0.78341
CVE-2014-0016	2014-03-24T16:31Z	2017-01-26T20:00Z	4.3	V2	0.00337	0.67615
CVE-2014-0017	2014-03-14T15:55Z	2014-03-26T04:55Z	1.9	V2	0.00042	0.05708
CVE-2014-0018	2014-02-14T15:55Z	2017-01-07T02:59Z	1.9	V2	0.00042	0.05708
CVE-2014-0019	2014-02-04T21:55Z	2018-10-30T16:27Z	1.9	V2	0.00042	0.05708

Questions?

TESORION

In case of **emergencies**

+31 88 27 47 800