David Gomes

CVEs

And the labeling problem

cve-search

cve-search

chat on gitter

Build & Test failing

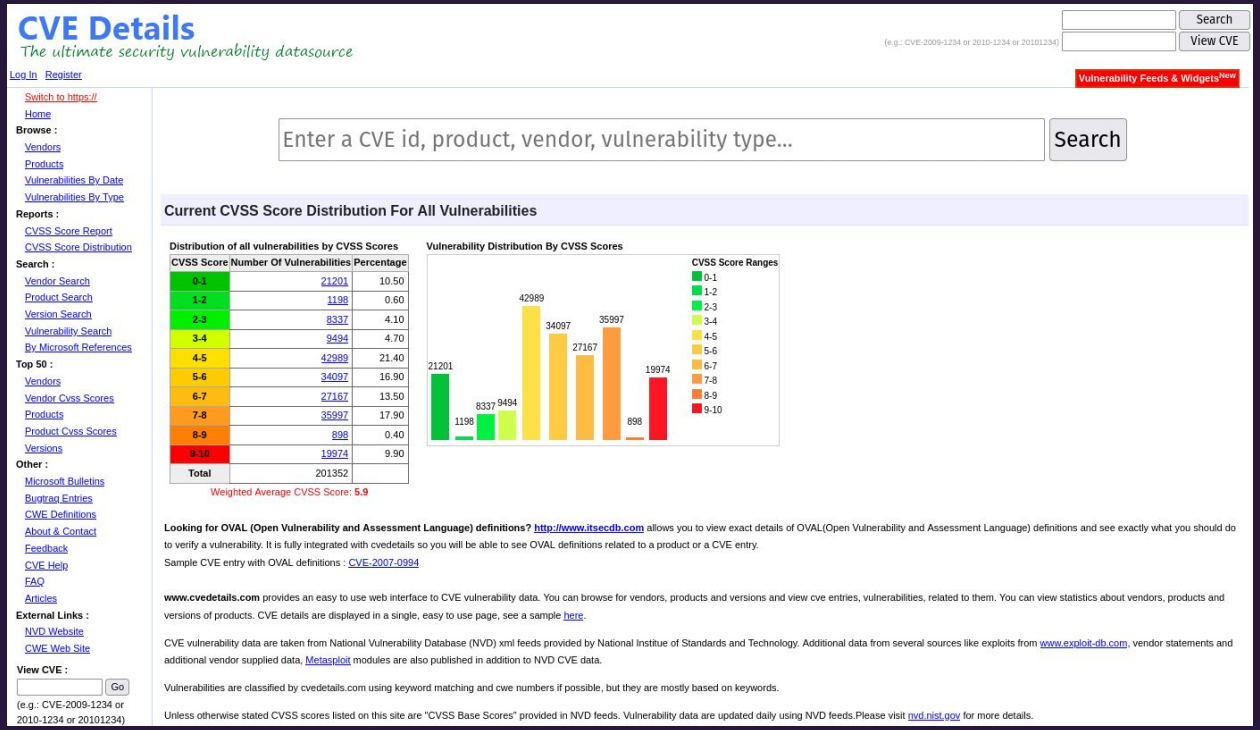
cve-search is a tool to import CVE (Common Vulnerabilities and Exposures) and CPE (Common Platform Enumeration) into a MongoDB to facilitate search and processing of CVEs.

The main objective of the software is to avoid doing direct and public lookups into the public CVE databases. Local lookups are usually faster and you can limit your sensitive queries via the Internet.

cve-search includes a back-end to store vulnerabilities and related information, an intuitive web interface for search and managing vulnerabilities, a series of tools to query the system and a web API interface.

cve-search is used by many organizations including the public CVE services of CIRCL.

cve-details


CVE Details
The ultimate security vulnerability datasource
Search
View CVE
Log In Register
Vulnerability Feeds & Widgets
Switch to https://
Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback
CVE Help
FAQ
Articles
External Links :
NVD Website
CWE Web Site
View CVE :
Go
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)
Enter a CVE id, product, vendor, vulnerability type...
Search
Current CVSS Score Distribution For All Vulnerabilities
Distribution of all vulnerabilities by CVSS Scores
CVSS Score | Number Of Vulnerabilities | Percentage
0-1 | 21201 | 10.50
1-2 | 1198 | 0.60
2-3 | 8337 | 4.10
3-4 | 9494 | 4.70
4-5 | 42989 | 21.40
5-6 | 34097 | 16.90
6-7 | 27167 | 13.50
7-8 | 35997 | 17.90
8-9 | 898 | 0.40
9-10 | 19974 | 9.90
Total | 201352
Weighted Average CVSS Score: 5.9
Vulnerability Distribution By CVSS Scores
CVSS Score Ranges
0-1
1-2
2-3
3-4
4-5
5-6
6-7
7-8
8-9
9-10
21201
1198
8337
9494
42989
34097
27167
35997
898
19974
Looking for OVAL (Open Vulnerability and Assessment Language) definitions? http://www.itsecdb.com allows you to view exact details of OVAL(Open Vulnerability and Assessment Language) definitions and see exactly what you should do to verify a vulnerability. It is fully integrated with cvedetails so you will be able to see OVAL definitions related to a product or a CVE entry.
Sample CVE entry with OVAL definitions : CVE-2007-0994
www.cvedetails.com provides an easy to use web interface to CVE vulnerability data. You can browse for vendors, products and versions and view cve entries, vulnerabilities, related to them. You can view statistics about vendors, products and versions of products. CVE details are displayed in a single, easy to use page, see a sample here.
CVE vulnerability data are taken from National Vulnerability Database (NVD) xml feeds provided by National Institue of Standards and Technology. Additional data from several sources like exploits from www.exploit-db.com, vendor statements and additional vendor supplied data, Metasploit modules are also published in addition to NVD CVE data.
Vulnerabilities are classified by cvedetails.com using keyword matching and cwe numbers if possible, but they are mostly based on keywords.
Unless otherwise stated CVSS scores listed on this site are "CVSS Base Scores" provided in NVD feeds. Vulnerability data are updated daily using NVD feeds.Please visit nvd.nist.gov for more details.

cve-details labels

- None
- Gain privileges
- Sql Injection
- Obtain Information
- Memory corruption
- CSRF
- Execute Code
- Denial Of Service
- Cross Site Scripting
- Http Response Splitting
- Directory traversal
- Bypass a restriction or something
- Overflow

Vulnerabilities By Type

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
1999	894	177	112	172			2	7		25	16	103			2
2000	1020	257	208	206	1	2	4	20		48	19	139			
2001	1677	403	403	297		7	34	124		83	36	220		2	2
2002	2156	498	553	435	2	41	200	103		127	76	199	2	14	1
2003	1527	381	477	372	2	50	129	60	1	62	69	144		16	5
2004	2451	580	614	408	3	148	291	111	12	145	96	134	5	38	5
2005	4935	838	1627	657	21	604	786	202	15	289	261	221	11	100	14
2006	6610	893	2719	666	91	967	1302	322	8	267	272	184	18	849	30
2007	6520	1101	2601	954	95	706	883	338	14	267	326	242	69	700	45
2008	5632	894	2310	699	128	1101	807	362	7	288	268	188	83	170	76
2009	5736	1035	2185	698	188	963	852	323	9	337	302	223	115	138	738
2010	4653	1102	1714	671	342	520	605	276	8	234	284	238	86	73	1501
2011	4155	1221	1334	723	351	294	470	109	7	197	408	206	58	17	557
2012	5297	1425	1459	828	423	243	759	122	13	344	391	250	166	14	623
2013	5191	1455	1186	846	366	155	650	110	7	352	510	274	123	1	206
2014	7939	1599	1572	839	420	304	1103	204	12	457	2107	239	264	2	403
2015	6504	1793	1830	1081	749	221	784	151	12	577	752	366	248	5	129
2016	6454	2028	1496	1219	717	94	498	99	15	444	866	601	86	7	1
2017	14714	3157	3004	2465	745	508	1518	278	11	629	1638	459	327	18	6
2018	16557	1855	3041	2120	400	517	2048	544	11	708	1227	247	461	31	4
2019	17344	1345	3201	1244	488	552	2391	475	10	712	913	202	535	57	13
2020	18325	1352	3251	1528	409	464	2183	415	14	966	1200	310	402	37	62
2021	20171	1838	3851	1660	483	741	2714	531	5	879	777	261	506	46	
2022	25227	2054	4064	2235	421	1789	3407	694	8	1056	680	216	744	54	
2023	8983	709	1618	696	137	765	1489	226	3	425	173	195	267	22	
Total	200672	29990	46430	23719	6982	11756	25909	6206	202	9918	13667	6061	4576	2411	4423
% Of All		14.9	23.1	11.8	3.5	5.9	12.9	3.1	0.1	4.9	6.8	3.0	2.3	1.2	

Android CVE data

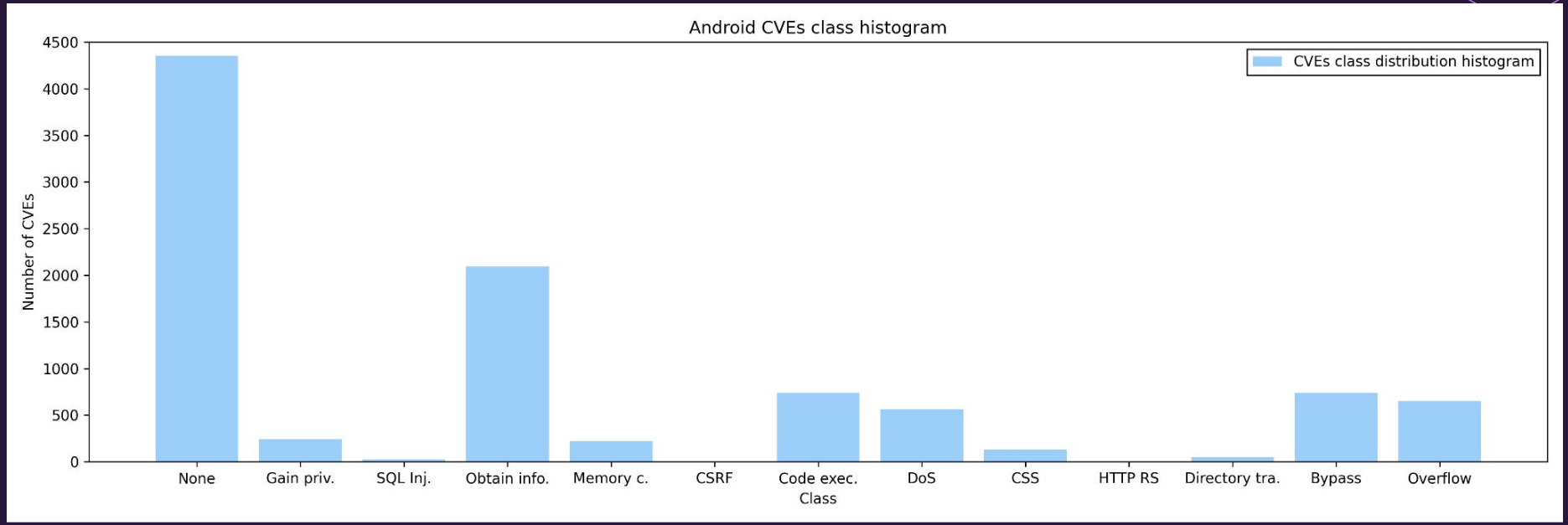
cves

	id	Published	Modified	summary	cvss	cwe	labels
0	CVE-2014-7552	2014-10-20T10:55:00.000Z	2014-11-14T14:13:00.000Z	The Zombie Diary (aka com.ezjoy.feelingtouch.z...	5.4	CWE-310	Obtain Information
1	CVE-2014-7745	2014-10-21T10:55:00.000Z	2014-11-14T14:17:00.000Z	The Flight Manager (aka com.flightmanager.view...	5.4	CWE-310	Obtain Information
2	CVE-2014-6661	2014-09-23T10:55:00.000Z	2014-09-26T15:55:00.000Z	The netease movie (aka com.netease.movie) appl...	5.4	CWE-310	Obtain Information
3	CVE-2014-5601	2014-09-09T01:55:00.000Z	2014-09-10T02:04:00.000Z	The 1800CONTACTS App (aka com.contacts1800.eco...	5.4	CWE-310	Obtain Information
4	CVE-2022-32550	2022-06-15T19:15:00.000Z	2022-06-24T17:27:00.000Z	An issue was discovered in AgileBits 1Password...	5.8	NVD-CWE-noinfo	None
...	...	...	...	...	...	...	...
9810	CVE-2016-6538	2018-07-06T21:29:00.000Z	2019-10-09T23:19:00.000Z	The TrackR Bravo mobile app stores the account...	3.3	CWE-200	None
9811	CVE-2016-6540	2018-07-06T21:29:00.000Z	2019-10-09T23:19:00.000Z	Unauthenticated access to the cloud-based serv...	3.3	CWE-200	Obtain Information
9812	CVE-2016-6541	2018-07-06T21:29:00.000Z	2019-10-09T23:19:00.000Z	TrackR Bravo device allows unauthenticated pai...	5.8	CWE-287	None
9813	CVE-2016-6539	2018-07-06T21:29:00.000Z	2019-10-09T23:19:00.000Z	The Trackr device ID is constructed of a manuf...	3.3	CWE-200	Obtain Information
9814	CVE-2020-13425	2020-05-23T20:15:00.000Z	2020-05-26T15:57:00.000Z	TrackR devices through 2020-05-06 allow attack...	6.8	CWE-862	Denial Of Service

Unlabeled CVEs

- CVEs with no label in the cve-details
- Objective: label the unlabeled CVEs summaries using Snorkel
- Some CVEs have multiple labels

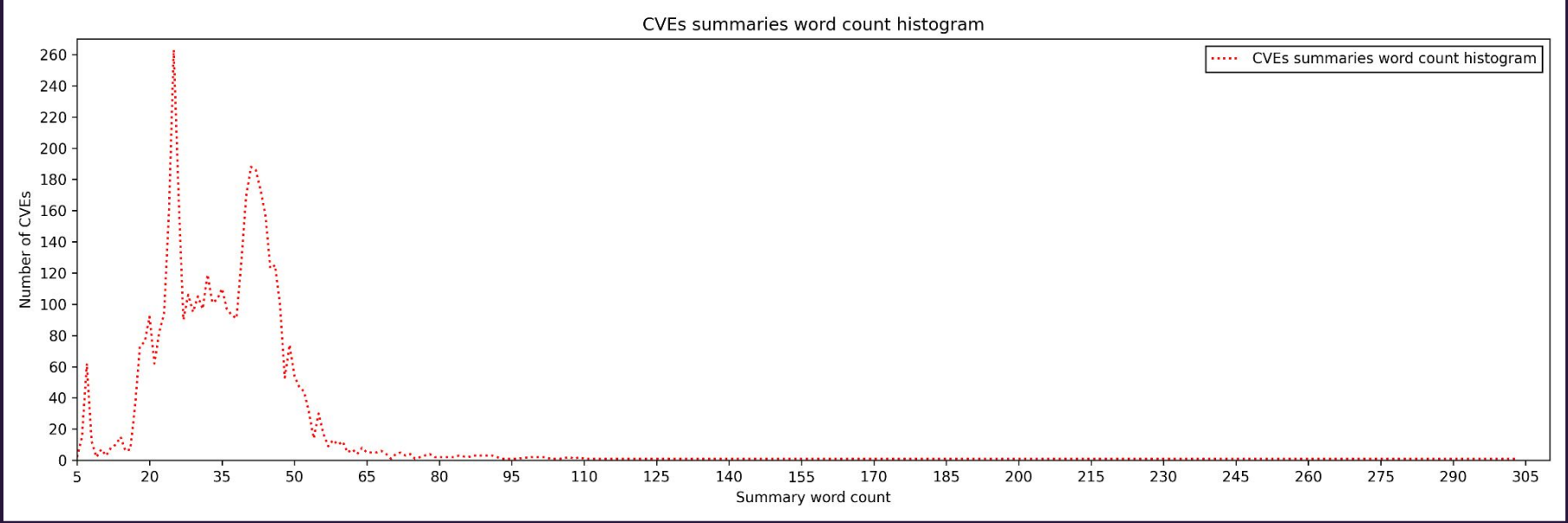
CVEs class histogram



35 most used words in unlabeled CVEs summaries

- the: 3278
- for: 2660
- user: 2052
- with: 2013
- this: 1930
- id: 1830
- android: 1822
- could: 1748
- lead: 1546
- there: 1532
- bounds: 1459
- privileges: 1455
- interaction: 1438
- prior: 1436
- execution: 1431
- needed.: 1428
- due: 1404
- needed: 1399
- not: 1397
- possible: 1377
- via: 1373
- attacker: 1372
- local: 1324
- remote: 1309
- and: 1291
- chrome: 1198
- androidversions:: 1119
- google: 1105
- allowed: 1094
- crafted: 1089
- information: 959
- additional: 923
- out: 876
- exploitation.product:: 864

Histogram


CVEs summaries word count histogram
CVEs summaries word count histogram
Number of CVEs
0
20
40
60
80
100
120
140
160
180
200
220
240
260
Summary word count
5
20
35
50
65
80
95
110
125
140
155
170
185
200
215
230
245
260
275
290
305

Examples of small unlabeled CVEs summaries

“Chromium: CVE-2021-30607 Use after free in Permissions”

“JetBrains YouTrack before 2020.3.5333 was vulnerable to SSRF.”

“Evernote prior to 5.5.1 has insecure password change”

“Unspecified vulnerabilities in Google Chrome before 54.0.2840.59.”

“Product: AndroidVersions: Android kernelAndroid ID: A-210936609References: N/A”

“Summary:Product: AndroidVersions: Android SoCAndroid ID: A-204686438”

“Android 1.0 through 9.0 has Insecure Permissions. The Android bug ID is 77286983.”

Examples of medium unlabeled CVEs summaries

“Use after free in Media in Google Chrome prior to 99.0.4844.51 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.”

“The Anti-theft service in AVG AntiVirus for Android allows physically proximate attackers to provide arbitrary location data via a "commonly available simple GPS location spoofer.”

“Insufficient data validation in JavaScript in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.”

“A race condition in Oilpan in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.”

Examples of medium unlabeled CVEs summaries

“Out of bounds write in WebRTC in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via crafted WebRTC packets.”

“iDrive RemotePC before 7.6.48 on Windows allows privilege escalation. A local and low-privileged user can force RemotePC to execute an attacker-controlled executable with SYSTEM privileges.”

“Incorrect default permissions in the Intel(R) Support Android application before version v22.02.28 may allow a privileged user to potentially enable information disclosure via local access.”

“In power management service, there is a missing permission check. This could lead to set up power management service with no additional execution privileges needed.”

“An elevation of privilege vulnerability in the Android framework (ui framework). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-35056974.”

Examples of medium unlabeled CVEs summaries

“server/LockSettingsService.java in LockSettingsService in Android 6.x before 2016-07-01 allows attackers to modify the screen-lock password or pattern via a crafted application, aka internal bug 28163930.”

“An issue was discovered on Samsung mobile devices with O(8.x) software. FactoryCamera does not properly restrict runtime permissions. The Samsung ID is SVE-2020-17270 (July 2020).”

“An issue was discovered on Samsung mobile devices with P(9.0) software. The Settings application allows unauthenticated changes. The Samsung IDs are SVE-2019-13814, SVE-2019-13815 (March 2019).”

“In startVideoStream() there is a possibility of an OOB Read in the heap, when the camera buffer is ‘zero’ in size.Product: AndroidVersions: Android-11Android ID: A-205097028”

Examples of big unlabeled CVEs summaries

“Product: Apache Cordova Android 5.2.2 and earlier. The application calls methods of the Log class. Messages passed to these methods (Log.v(), Log.d(), Log.i(), Log.w(), and Log.e()) are stored in a series of circular buffers on the device. By default, a maximum of four 16 KB rotated logs are kept in addition to the current log. The logged data can be read using Logcat on the device. When using platforms prior to Android 4.1 (Jelly Bean), the log data is not sandboxed per application; any application installed on the device has the capability to read data logged by other applications.”

“A vulnerability in the user interface of Cisco Webex Meetings and Cisco Webex Meetings Server Software could allow an authenticated, remote attacker to inject a hyperlink into a meeting invitation email. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by entering a URL into a field in the user interface. A successful exploit could allow the attacker to generate a Webex Meetings invitation email that contains a link to a destination of their choosing. Because this email is sent from a trusted source, the recipient may be more likely to click the link.”

Examples of big unlabeled CVEs summaries

“The 'Copy Image Link' context menu action would copy the final image URL after redirects. By embedding an image that triggered authentication flows - in conjunction with a Content Security Policy that stopped a redirection chain in the middle - the final image URL could be one that contained an authentication token used to takeover a user account. If a website tricked a user into copy and pasting the image link back to the page, the page would be able to steal the authentication tokens. This was fixed by making the action return the original URL, before any redirects. This vulnerability affects Firefox < 94.”

“Microsoft introduced a new feature in Windows 10 known as Cloud Clipboard which, if enabled, will record data copied to the clipboard to the cloud, and make it available on other computers in certain scenarios. Applications that wish to prevent copied data from being recorded in Cloud History must use specific clipboard formats; and Firefox before versions 94 and ESR 91.3 did not implement them. This could have caused sensitive data to be recorded to a user's Microsoft account. *This bug only affects Firefox for Windows 10+ with Cloud Clipboard enabled. Other operating systems are unaffected.*. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3.”

Example of big unlabeled CVE summary

“Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 6u141, 7u131 and 8u121; Java SE Embedded: 8u121; JRockit: R28.3.13. Difficult to exploit vulnerability allows unauthenticated attacker with network access via SMTP to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded, JRockit accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).”

Example of big unlabeled CVE summary

“A vulnerability has been identified in SIMATIC WinCC OA UI for Android (All versions < V3.15.10), SIMATIC WinCC OA UI for iOS (All versions < V3.15.10). Insufficient limitation of CONTROL script capabilities could allow read and write access from one HMI project cache folder to other HMI project cache folders within the app's sandbox on the same mobile device. This includes HMI project cache folders of other configured WinCC OA servers. The security vulnerability could be exploited by an attacker who tricks an app user to connect to an attacker-controlled WinCC OA server. Successful exploitation requires user interaction and read/write access to the app's folder on a mobile device. The vulnerability could allow reading data from and writing data to the app's folder. At the time of advisory publication no public exploitation of this security vulnerability was known. Siemens confirms the security vulnerability and provides mitigations to resolve the security issue.”

Example of big unlabeled CVE summary

“On some Samsung phones and tablets running Android through 7.1.1, it is possible for an attacker-controlled Bluetooth Low Energy (BLE) device to pair silently with a vulnerable target device, without any user interaction, when the target device's Bluetooth is on, and it is running an app that offers a connectable BLE advertisement. An example of such an app could be a Bluetooth-based contact tracing app, such as Australia's COVIDSafe app, Singapore's TraceTogether app, or France's TousAntiCovid (formerly StopCovid). As part of the pairing process, two pieces (among others) of personally identifiable information are exchanged: the Identity Address of the Bluetooth adapter of the target device, and its associated Identity Resolving Key (IRK). Either one of these identifiers can be used to perform re-identification of the target device for long term tracking. The list of affected devices includes (but is not limited to): Galaxy Note 5, Galaxy S6 Edge, Galaxy A3, Tab A (2017), J2 Pro (2018), Galaxy Note 4, and Galaxy S5.”

Example of big unlabeled CVE summary

“matrix-android-sdk2 is the Matrix SDK for Android. Prior to version 1.5.1, an attacker cooperating with a malicious homeserver can construct messages that legitimately appear to have come from another person, without any indication such as a grey shield. Additionally, a sophisticated attacker cooperating with a malicious homeserver could employ this vulnerability to perform a targeted attack in order to send fake to-device messages appearing to originate from another user. This can allow, for example, to inject the key backup secret during a self-verification, to make a targeted device start using a malicious key backup spoofed by the homeserver. matrix-android-sdk2 would then additionally sign such a key backup with its device key, spilling trust over to other devices trusting the matrix-android-sdk2 device. These attacks are possible due to a protocol confusion vulnerability that accepts to-device messages encrypted with Megolm instead of Olm. matrix-android-sdk2 version 1.5.1 has been modified to only accept Olm-encrypted to-device messages and to stop signing backups on a successful decryption. Out of caution, several other checks have been audited or added. This attack requires coordination between a malicious home server and an attacker, so those who trust their home servers do not need a workaround.”

The biggest unlabeled CVE summary (303 words)

“A vulnerability was discovered in the Zoom Client for Meetings (for Android, iOS, Linux, macOS, and Windows) before version 5.8.4, Zoom Client for Meetings for Blackberry (for Android and iOS) before version 5.8.1, Zoom Client for Meetings for intune (for Android and iOS) before version 5.8.4, Zoom Client for Meetings for Chrome OS before version 5.0.1, Zoom Rooms for Conference Room (for Android, AndroidBali, macOS, and Windows) before version 5.8.3, Controllers for Zoom Rooms (for Android, iOS, and Windows) before version 5.8.3, Zoom VDI Windows Meeting Client before version 5.8.4, Zoom VDI Azure Virtual Desktop Plugins (for Windows x86 or x64, IGEL x64, Ubuntu x64, HP ThinPro OS x64) before version 5.8.4.21112, Zoom VDI Citrix Plugins (for Windows x86 or x64, Mac Universal Installer & Uninstaller, IGEL x64, eLux RP6 x64, HP ThinPro OS x64, Ubuntu x64, CentOS x 64, Dell ThinOS) before version 5.8.4.21112, Zoom VDI VMware Plugins (for Windows x86 or x64, Mac Universal Installer & Uninstaller, IGEL x64, eLux RP6 x64, HP ThinPro OS x64, Ubuntu x64, CentOS x 64, Dell ThinOS) before version 5.8.4.21112, Zoom Meeting SDK for Android before version 5.7.6.1922, Zoom Meeting SDK for iOS before version 5.7.6.1082, Zoom Meeting SDK for macOS before version 5.7.6.1340, Zoom Meeting SDK for Windows before version 5.7.6.1081, Zoom Video SDK (for Android, iOS, macOS, and Windows) before version 1.1.2, Zoom on-premise Meeting Connector before version 4.8.12.20211115, Zoom on-premise Meeting Connector MMR before version 4.8.12.20211115, Zoom on-premise Recording Connector before version 5.1.0.65.20211116, Zoom on-premise Virtual Room Connector before version 4.4.7266.20211117, Zoom on-premise Virtual Room Connector Load Balancer before version 2.5.5692.20211117, Zoom Hybrid Zproxy before version 1.0.1058.20211116, and Zoom Hybrid MMR before version 4.6.20211116.131_x86-64 which potentially allowed for the exposure of the state of process memory. This issue could be used to potentially gain insight into arbitrary areas of the product's memory.”

Thanks!