STORM WATCH

CYBERSECURITY NEWS

Dateline: 2024-06-25

LIKE

SUBSCRIBE

Storm ⚡ Watch by GreyNoise Intelligence

GreyNoise Intelligence

TECHNOLOGY · UPDATED WEEKLY

GreyNoise Storm ⚡ Watch is a weekly podcast and livestream hosted by GreyNoise Intelligence (https://www.greynoise.io), a cybersecurity company that focuses on understanding internet noise. The show features hosts b MORE

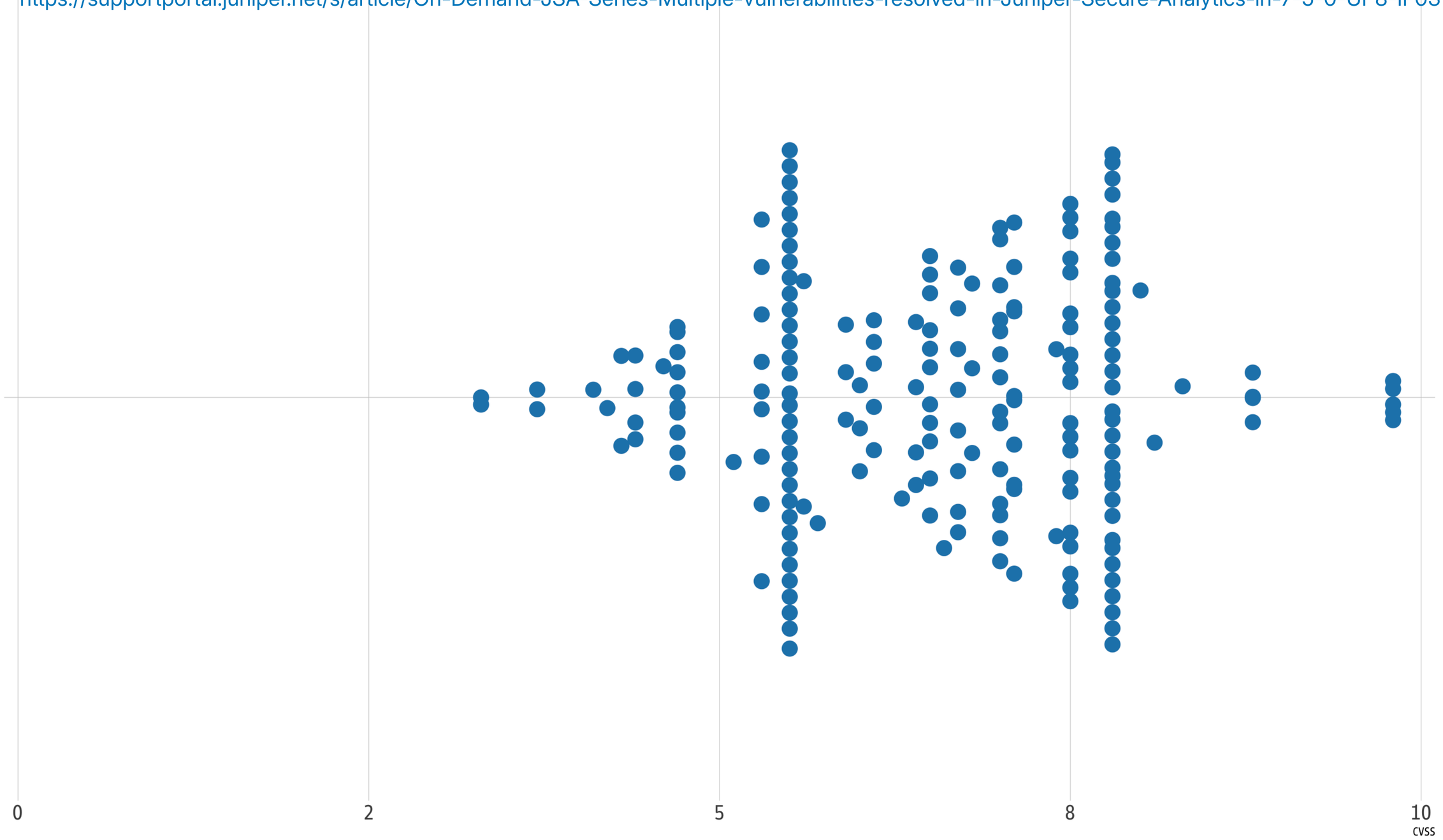
https://StormWatch.ing

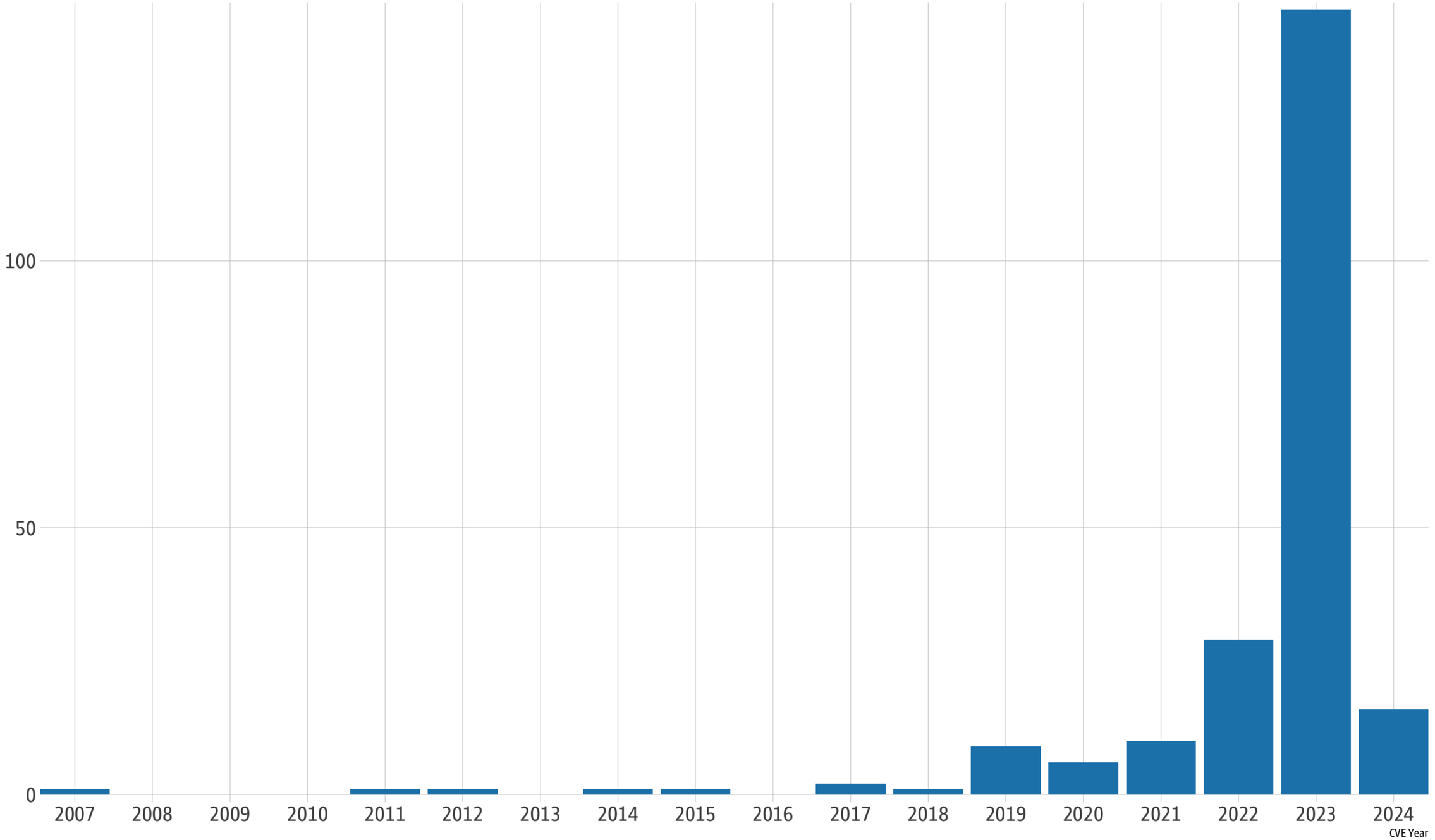
LEAVE A COMMENT

SHARE


BREAKING
NEWS

https://supportportal.juniper.net/s/article/On-Demand-JSA-Series-Multiple-vulnerabilities-resolved-in-Juniper-Secure-Analytics-in-7-5-0-UP8-IF03




100
50
0
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
CVE Year

CVE	CVSS	Summary
CVE-2019-19012	9.8	An integer overflow in the search_in_range function in regexec.c in Oniguruma 6.x before 6.9.4_rc2 leads to an out-of-bounds read, in which the offset of this read is under the control of an attacker. (This only affects the 32-bit compiled version). Remote attackers can cause a denial-of-service or information disclosure, or possibly have unspecified other impact, via a crafted regular expression.
CVE-2023-5178	9.8	A use-after-free vulnerability was found in drivers/nvme/target/tcp.c` in `nvmet_tcp_free_crypto` due to a logical bug in the NVMe/TCP subsystem in the Linux kernel. This issue may allow a malicious user to cause a use-after-free and double-free problem, which may permit remote code execution or lead to local privilege escalation.
CVE-2019-15505	9.8	drivers/media/usb/dvb-usb/technisat-usb2.c in the Linux kernel through 5.2.9 has an out-of-bounds read via crafted USB device traffic (which may be remote via usbip or usbredir).
CVE-2023-40547	8.3	A remote code execution vulnerability was found in Shim. The Shim boot support trusts attacker-controlled values when parsing an HTTP response. This flaw allows an attacker to craft a specific malicious HTTP request, leading to a completely controlled out-of-bounds write primitive and complete system compromise. This flaw is only exploitable during the early boot phase, an attacker needs to perform a Man-in-the-Middle or compromise the boot server to be able to exploit this vulnerability successfully.
CVE-2023-52434	8.0	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix potential OOBs in smb2_parse_contexts() Validate offsets and lengths before dereferencing create contexts in smb2_parse_contexts(). This fixes following oops when accessing invalid create contexts from server: BUG: unable to handle page fault for address: ffff8881178d8cc3 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 4a01067 P4D 4a01067 PUD 0 Oops: 0000 [#1] PREEMPT SMP NOPTI CPU: 3 PID: 1736 Comm: mount.cifs Not tainted 6.7.0-rc4 #1 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS rel-1.16.2-3-gd478f380-rebuilt.opensuse.org 04/01/2014 RIP: 0010:smb2_parse_contexts+0xa0/0x3a0 [cifs] Code: f8 10 75 13 48 b8 93 ad 25 50 9c b4 11 e7 49 39 06 0f 84 d2 00 00 00 8b 45 00 85 c0 74 61 41 29 c5 48 01 c5 41 83 fd 0f 76 55 <0f> b7 7d 04 0f b7 45 06 4c 8d 74 3d 00 66 83 f8 04 75 bc ba 04 00 RSP: 0018:ffffc900007939e0 EFLAGS: 00010216 RAX: ffffc90000793c78 RBX: ffff8880180cc000 RCX: ffffc90000793c90 RDX: ffffc90000793cc0 RSI: ffff8880178d8cc0 RDI: ffff8880180cc000 RBP: ffff8881178d8cbf R08: ffffc90000793c22 R09: 0000000000000000 R10: ffff8880180cc000 R11: 0000000000000024 R12: 0000000000000000 R13: 0000000000000020 R14: 0000000000000000 R15: ffffc90000793c22 FS: 00007f873753cbc0(0000) GS:ffff88806bc00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: ffff8881178d8cc3 CR3: 00000000181ca000 CR4: 0000000000750ef0 PKRU: 55555554 Call Trace: <TASK> ? __die+0x23/0x70 ? page_fault_oops+0x181/0x480 ? search_module_extables+0x19/0x60 ? srso_alias_return_thunk+0x5/0xfbef5 ? exc_page_fault+0x1b6/0x1c0 ? asm_exc_page_fault+0x26/0x30 ? smb2_parse_contexts+0xa0/0x3a0 [cifs] SMB2_open+0x38d/0x5f0 [cifs] ? smb2_is_path_accessible+0x138/0x260 [cifs] smb2_is_path_accessible+0x138/0x260 [cifs] cifs_is_path_remote+0x8d/0x230 [cifs] cifs_mount+0x7e/0x350 [cifs] cifs_smb3_do_mount+0x128/0x780 [cifs] smb3_get_tree+0xd9/0x290 [cifs] vfs_get_tree+0x2c/0x100 ? capable+0x37/0x70 path_mount+0x2d7/0xb80 ? srso_alias_return_thunk+0x5/0xfbef5 ? _raw_spin_unlock_irqrestore+0x44/0x60 __x64_sys_mount+0x11a/0x150 do_syscall_64+0x47/0xf0 entry_SYSCALL_64_after_hwframe+0x6f/0x77 RIP: 0033:0x7f8737657b1e

```
> grep("linux kernel", gsub("[\n\r]", "", xdf$Summary), ignore.case = TRUE)
  [1]  17  19  20  21  22  23  24  25  26  28  29  30  31  32  33  34  38  39
 [19]  40  41  42  43  44  45  46  47  48  49  51  52  53  54  56  57  59  60
 [37]  61  62  65  66  67  68  70  71  72  73  76  77  78  79  81  82  83  84
 [55]  85  86  88  90  91  92  93  94  95  96  97  99 101 102 103 104 107 108
 [73] 109 112 113 114 115 116 117 118 119 120 121 122 123 124 125 169 170 171
 [91] 172 173 174 175 176 177 181 182 183 184 185 186 187 188 189 190 191 192
[109] 193 194 195 196 197 199 200 201 202 203 204 205 206 207 208 209 210 211
[127] 212 213 215
```

STORM WATCH

CYBERSECURITY NEWS

OpenSSF

OPEN SOURCE SECURITY FOUNDATION

https://openssf.org/blog/2024/05/20/enhancing-open-source-security-introducing-siren-by-openssf/

The OpenSSF Siren is a collaborative effort to aggregate and disseminate threat intelligence specific to open source projects. Hosted by the OpenSSF, this platform provides a secure and transparent environment for sharing Tactics, Techniques, and Procedures (TTPs) and Indicators of Compromise (IOCs) associated with recent cyber attacks. Siren is intended to be a post-disclosure means of keeping the community informed of threats and activities after the initial sharing and coordination.

Open Source Threat Intelligence: shared with the community about actively exploited public vulnerabilities and threats.

Real-Time Updates: List members receive notifications via email about emerging threats which may be relevant to their projects, enabling swift action to mitigate risks.

TLP:CLEAR: To facilitate effective unrestricted transparent communication, the list follows the Traffic Light Protocol (TLP), Clear guidelines for the sharing and handling of intelligence.

Community-driven: Contributors from diverse backgrounds collaborate to enrich the intelligence database, fostering a culture of shared responsibility and collective defense.

STORM WATCH

CYBERSECURITY NEWS

SHAMELESS SELF-PROMOTION

VULNERABILITIES LABS

SolarWinds Serv-U (CVE-2024-28995) exploitation: We see you!

Ron Bowes | June 18, 2024

https://www.greynoise.io/blog/solarwinds-serv-u-cve-2024-28995-exploitation-we-see-you

STORM WATCH

CYBERSECURITY NEWS

TAG ROUND-UP

Apache NiFi RCE Scanner

FatPipe WARP 10.2.2 Authorization Bypass Scanner

FatPipe WARP 10.2.2 Authorization Bypass Attempt

Zyxel CVE-2024-29973 RCE Attempt

WE NEED

TO TALK

ABOUT

KEV

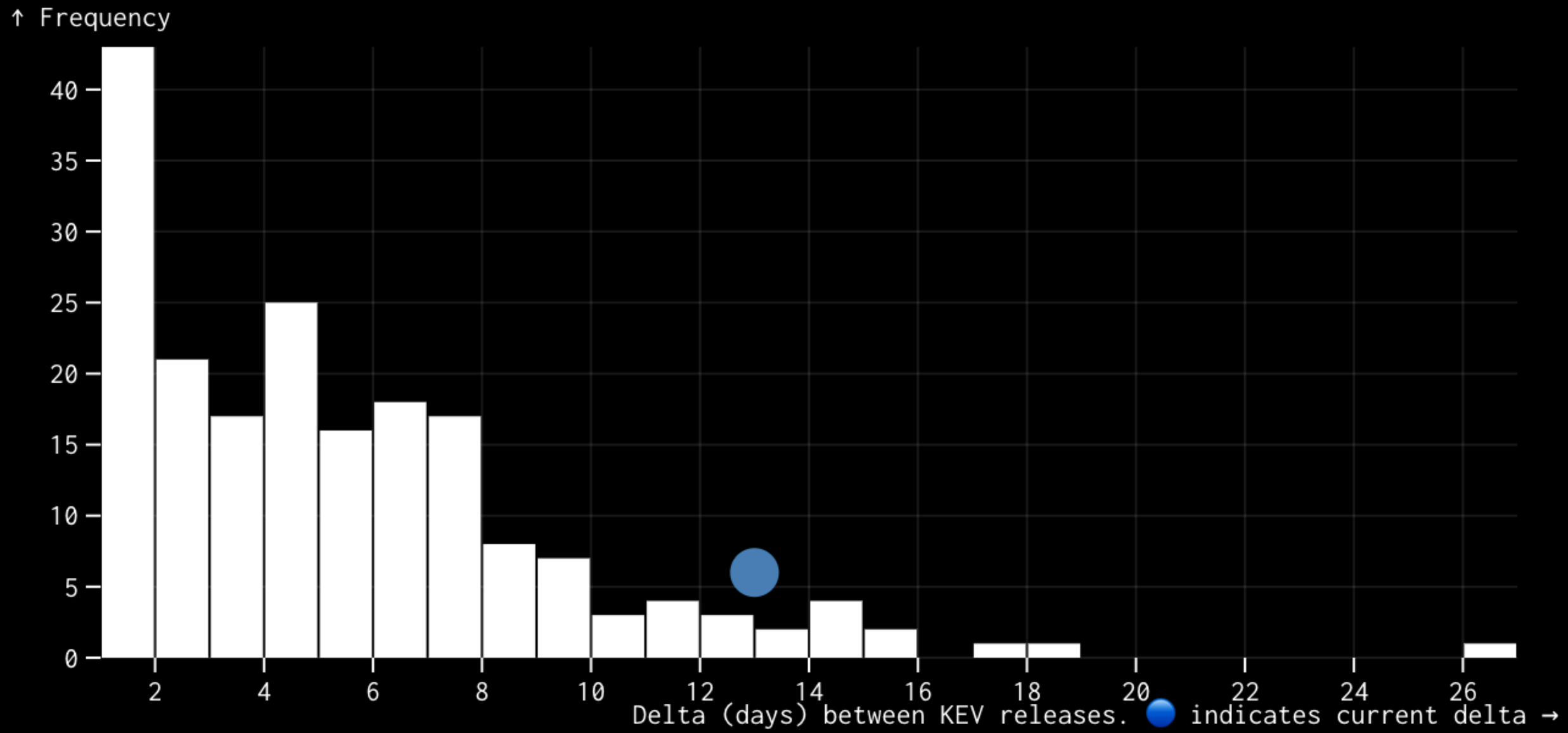
STORM WATCH

It Has Been

12

Days Since The Last KEV Release

https://kev.hrbrmstr.app


↑ Frequency
40
35
30
25
20
15
10
5
0
2
4
6
8
10
12
14
16
18
20
22
24
26
Delta (days) between KEV releases. indicates current delta →