zxcvbn algorithmic complexity attack

Submitted about 16 hours ago

Status

Not applicable

This submission was marked not applicable. It is not a rewardable submission at this time.

Reward

version

1.10.1 (/vulnerability-rating-taxonomy/1.10.1)

Program

Dropbox (/dropbox)

Closed on

9 Feb 2023

CrowdStream visibility

Choose to associate your details with this submission in CrowdStream when accepted.

Please note that your username will always be shown against your submission if it is disclosed.

Show username

Show reward

Please note: This program does not currently disclose submission activity in CrowdStream.

ID

`c18936f3-c31e-4238-a3b0-30d4258ee1ec`

Reference

Support

`70f2e59eb8aee3c67cbfe11300fb765416d2556d941b0b799714d3c92400da4b` Deprecated

Submitted

08 Feb 2023 23:01:21 UTC

Target Location

Target category

Unspecified

VRT (VULNERABILITY RATING TAXONOMY)

Application-Level Denial-of-Service (DoS) > Critical Impact and/or Easy Difficulty

Priority

P2 Suggested priority based on the identified VRT

Bug URL

https://github.com/GoSimpleLLC/nbvcxz/issues/60

Description

Support

This DOS has not been tested against your specific services as I don't believe they are vulnerable. Instead, a library that you maintain (Zxcvbn) and the algorithms it implements are the vulnerability target, when used in different contexts than Dropbox uses them.

Please see attached writeup my employer approved after I made them aware and had patched our software: [zxcvbn-denial-of-service-bug-report.pdf].

The research originally published a company (Two Six Technologies) in close proximity to the US Government has been incorporated into exploits that are in at least somewhat widespread use, beyond the NSA. Downstream software that implements these algorithms and runs server-side without additional precautions is at risk. I have received reports from users of my library that successful denial-of-service (DoS) attacks have been carried out against products using these methods. I have proven those same methods were applicable against your library when run server-side. The issue has gone unaddressed for multiple years, even after I originally found mention of it (and opened an issue but did not look into it until recently). I have been unable to reach the original maintainer, who is no longer employed by your company, to resolve this issue. It is critical that a maintainer is assigned to this project, as it represents your corporate brand and is widely used within the industry at this point.

1 - Please see direct the bug report for zxcvbn here: https://github.com/dropbox/zxcvbn/issues/326

2 - Here is the original pickup of the exploit, and the central issue for tracking getting all the ports patched: https://github.com/GoSimpleLLC/nbvcxz/issues/60

3 - This release of my port fixed the issue for my library: https://github.com/GoSimpleLLC/nbvcxz/releases/tag/1.5.1

4 - Me trying to reach out through HN prior to finding this avenue: https://news.ycombinator.com/item?id=34540783

5 - Reporting about this exploit back in 2019: https://www.engadget.com/2019-08-09-new-ddos-attack-algorithms.html

6 - Original blackhat conf presentation attached [us-19-Hauke-Denial-Of-Service-With-A-Fistful-Of-Packets-Exploiting-Algorithmic-Complexity-Vulnerabilities.pdf]

7 - Additional report of the ReDoS exploit mentioned: https://github.com/dropbox/zxcvbn/issues/327

Files attached

- us-19-Hauke-Denial-Of-Service-With-A-Fistful-Of-Packets-Exploiting-Algorithmic-Complexity-Vulnerab…
- zxcvbn-denial-of-service-bug-report.pdf (610 KB) (/attachments/znrbkmnnoy)

Disclose report to CrowdStream

Support

Open a request to disclose this report to CrowdStream (/crowdstream). We recommend reques

after the vulnerability is marked as resolved.

Disclosure requests **will not speed up** submission transition.

Please review our Public Disclosure Policy (https://docs.bugcrowd.com/researchers/reporting-managing-submissions/disclosure/disclosing-submissions/) before submitting a request.

Request disclosure

Activity

Tostino created the submission

16 hours ago

sophie_bugcrowd sent a message

9 hours ago

Hi Tostino,

We appreciate your work on this submission, however, this type of issue is specifically listed as Out of Scope. Please carefully re-read the brief:bounty brief (https://www.bugcrowd.com/dropbox)

> Issues that result in Denial of Service (DoS) to Dropbox's servers at the network or application layer

Best regards,
- sophie_bugcrowd

sophie_bugcrowd changed the state to **Not applicable**

9 hours ago

Support

Tostino sent a message

in a few seconds • Notification email sent

Sophie,

I didn't spend my time on this for the meagre monetary compensation. I read the bounty brief. That is why I prefaced the message with the fact that I don't believe the Dropbox services are vulnerable due to the way you integrate the library. It's that your company "maintains" a vulnerable library that is widely used by industry and no one that works there seems to be interested in fixing it.

I eagerly await your less condescending response.

Thanks,
-Adam Brusselback

Terms & Conditions (https://www.bugcrowd.com/terms-and-conditions)

Privacy Policy (https://www.bugcrowd.com/privacy)

Do not sell my information (https://www.bugcrowd.com/privacy/do-not-sell-my-information/)

Docs (https://docs.bugcrowd.com/researchers/onboarding/welcome)
FAQ (https://www.bugcrowd.com/resources/for-researchers/faqs)
Resources (https://www.bugcrowd.com/resources/for-researchers)
Private Crowd (https://www.bugcrowd.com/resource/help-wanted) Careers (https://www.bugcrowd.com/about/careers)

Support