Gmail nu11 secur1ty <[redacted]>

96.0.4664.110-Stacktrace

4 съобщения

nu11 secur1ty <[redacted]> 22 януари 2022 г., 8:56 ч.
До: security@chromium.org

https://github.com/nu11secur1ty/CVE-nu11secur1ty/tree/main/vendors/Microsoft/2022/chrome%3D96.0.4664.110-Stacktrace

--

System Administrator - Infrastructure Engineer
Penetration Testing Engineer
Exploit developer at https://packetstormsecurity.com/ https://cve.mitre.org/index.html and https://www.exploit-db.com/
home page: https://www.nu11secur1ty.com/
hiPEnIMR0v7QCo/+SEH9gBclAAYWGnPoBIQ75sCj60E=
nu11secur1ty

Chris Bookholt <bookholt@google.com> 23 януари 2022 г., 0:26 ч.
До: nu11 secur1ty <[redacted]>
Як: security@chromium.org

Hi there, thanks for getting in touch!

From what I can see in the screen recording, it looks like the crash originates in the Selenium WebDriver due to DNS resolution failure. It happens very quickly in the recording, but it looks like the hostname entered into Chrome's Omnibar is all As, in which case the name resolution failure makes sense. The DNS failure leads to a Python exception that produces a stack trace of the Python process and then terminates the associated process tree.

We would be happy to take a closer look if you would like to share an unencrypted proof-of-concept. If the bug is suspected to be in Chrome then it is most helpful if you can share a POC that does not require third party software like Selenium. The best way to report bugs in Chrome is through our bug tracker using the process described at https://www.chromium.org/Home/chromium-security/reporting-security-bugs

If you feel the bug is in Selenium, the best place to report those bugs is in their project issue tracker.

Thanks again for taking the time to get in touch, all the best!
Chris Bookholt | Security Engineer | bookholt@google.com | +1 (425) 655-4364

[Цитираният текст е скрит]

> [Цитираният текст е скрит]
> --
> --
> -----
> security@chromium.org is for discussing vulnerabilities and fixes in Chromium code.
> Please protect Chromium users: DO NOT FORWARD this email or disclose its contents to third parties.
>
> http://groups.google.com/a/chromium.org/group/security
>
> ---
> To unsubscribe from this group and stop receiving emails from it, send an email to security+unsubscribe@chromium.org.

nu11 secur1ty [redacted] 23 януари 2022 г., 10:18 ч.
До: Chris Bookholt <bookholt@google.com>
Як: security@chromium.org

Thank you for your response. It's Done
Actually, this is a fake request and you must make a correctly checking for it if you don't have the correct connection > just close and kill the request ;)
KR
[Цитираният текст е скрит]

---

nu11 secur1ty [redacted] 23 януари 2022 г., 10:27 ч.
До: Chris Bookholt <bookholt@google.com>

Yes, this is a request from selenium. So it is not so big problem for me, but it is a problem =)
KR dear friend!
[Цитираният текст е скрит]