

Forum:[Hack Forums](#)

Thread: [Careful with the new Oday. ALERT](#)

Mr. Robot - April 15, 2023, 5:38 pm

CVE-2023-2033

Already seen people tryna execute this in the wild.

Edge and Chrome users beware - I think it can also be popped via discord in browser.

Long story short all that has been disclosed:

"A remote attacker could exploit this Chrome V8 type confusion vulnerability to cause heap corruption via a crafted HTML page"

Based on that information we can tell that it's to do with the way JavaScript code is executed. This is common in things like Node.js, but due to the way the Chrome V8 JavaScript engine is used, it affected other browsers too such as Brave and Opera.

What we know so far is that it might have been able to affect Discord as well based on the dependencies, however this is unknown at this time due to the way it displays data.

What this exploit takes advantage of is a "type confusion" which is when the javascript engine incorrectly associates the type of an object or code in memory such as an integer or string. Because of how JavaScript works and the fact it's a dynamically typed language, variables can change type WHILE being executed but while they change type, at run time the engine needs to keep track of which type is which.

This allows more control over the memory of the javascript engine - if you can make the engine during run time execute extra data in memory, in this case making it think it's running one type such as an integer vs a string, it would perform incorrect operations on the output object or what is displayed/run in the browsers end.

Example javascript of an integer and a string

Code // Integer example

```
let integerExample = 123;
```

// String example

```
let stringExample = "This is a string";
```

From here you can leverage the object left in memory and store objects leading to a heap corruption. From a heap corruption you can possible expose information or cause arbitrary code execution.

A heap corruption in short is when there is a memory issue on a website and the heap which is a locally stored area on your machine for your browser is used for storing information during runtime is caused to run outside that allocated space, giving access to areas that are persistent and not deleted after runtime.

Using this information we can see that an attacker would make the HTML page containing javascript code that triggers the type confusion, specifically targeting the V8 engine. Anyone who visits the website would have their browsers memory heap corrupted which could then lead to code execution or exposure of local files/data.

TLDR:

1. You have a heap file/location that is edited during runtime. It's unloaded and loaded when your browser is open/when the javascript is running on a site.
2. A malicious website can take advantage of that by causing an error in the way javascript is run, meaning that heap location 'falls apart' and extra code is placed outside of it for persistence.
3. That code outside of the heap is no longer 'sandboxed' the same way which can lead to information being sent back to the user/code being executed.

Mr. Robot - April 15, 2023, 6:31 pm

(Apr 15, 2023 06:24 PM)Animal Wrote: [\[CITE\]](#) Thanks for the alert. It's real deal, Google Chrome has rolled out an urgent update to fix a zero-day bug that was being abused. You all need to update your browser to version 112.0.5615.121 asap.

A lot of browsers use the same chromium versions like Brave, Opera, etc

source - April 15, 2023, 8:52 pm

"Type confusion in V8 in Google Chrome prior to 112.0.5615.121 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page," according to the NIST's National Vulnerability Database (NVD).

<https://nvd.nist.gov/vuln/detail/CVE-2023-2033>

Aadgjmpw72 - April 15, 2023, 9:06 pm

Anyone have more details on this? maybe a POC?

spiderman6942069 - April 15, 2023, 9:42 pm

Thanks for the heads up

B3A - April 16, 2023, 1:52 am

(Apr 15, 2023 09:17 PM)m0hx Wrote: [\[CITE\]](#) Can someone explain what does it do exactly?
I'll stay here aswell till i find out

Mr. Robot - April 16, 2023, 1:59 am

(Apr 15, 2023 09:17 PM)m0hx Wrote: [\[CITE\]](#) Can someone explain what does it do exactly?
Did you actually want a run down or were you meming. I couldn't tell sorry

{ RadioActive Hack } - April 16, 2023, 2:22 am

I've hear about this Oday before, but I don't really know much about it. Just that it's a big deal.

Does anyone have a link to a thread or resource to check it out?

Thanks. <3

Gody - April 16, 2023, 3:56 am

Thanks but I need the POC !

Mac Miller - April 16, 2023, 4:18 am

Anyone gotta explain exactly what this Oday does

Mr. Robot - April 16, 2023, 4:32 am

(Apr 16, 2023 04:18 AM)Mac Miller Wrote: [\[CITE\]](#) Anyone gotta explain exactly what this Oday does
I'll do a writeup soon just busy on some shit right now.

Mac Miller - April 16, 2023, 5:26 am

(Apr 16, 2023 04:32 AM)Mr. Robot Wrote: [\[CITE\]](#) I'll do a writeup soon just busy on some shit right now.

Bet bet thank you even the official CVE listing doesn't say much

javierpena - April 16, 2023, 6:49 am

Posting to understand what heap corruption means. Also I am using Brave on Fedora and it tells me I have the latest Chromium update with 111.0.55xxxx is it because I am on Linux? If not how to update?

Grim - April 16, 2023, 2:06 pm

saw this on my friends browser was about to post it as well but thanks for the heads up.

oRequiem - April 16, 2023, 2:16 pm

Had no idea about this one, thanks for the heads up.

B3A - April 17, 2023, 7:35 am

(Apr 16, 2023 04:32 AM)Mr. Robot Wrote: [\[CITE\]](#) I'll do a writeup soon just busy on some shit right now.

I'll be here waiting .

Add a multi-quote for all us noobs please. ?

Laughing Man - April 17, 2023, 8:15 am

Man exploits have been going nuts these last 4-5 years.

I remember when bug bounty programs actually had use and shit got patched hella fast.

Ph4n70M Phr34K - April 17, 2023, 8:26 am

Good to see google reacting fast to this. Anyone has some articles proving this vulnerability was used in actual attack ?

Laughing Man - April 17, 2023, 8:28 am

(Apr 17, 2023 08:26 AM)Ph4n70M Phr34K Wrote: [\[CITE\]](#) Good to see google reacting fast to this. Anyone has some articles proving this vulnerability was used in actual attack ?

Let's see how long it takes for Brave/FF to catch up.

BiNBo - April 17, 2023, 10:25 am

This came up in my Monday morning meeting, I immediately pushed the update to all of my affected users. Almost all of these that come up are, but this is a particularly nasty 0day for sure.

AiDenti - April 17, 2023, 1:12 pm

Good to know. Anyone wanna explain how this works?

Stunner - April 17, 2023, 2:03 pm

Thanks a lot for the heads up

B3A - April 17, 2023, 2:03 pm

(Apr 17, 2023 01:12 PM)AiDenti Wrote: [\[CITE\]](#) Good to know. Anyone wanna explain how this works?

Im staying here waiting for the same thing?

Goldstream - April 17, 2023, 6:33 pm

Thanks! For the heads up man will be updating

B3A - April 19, 2023, 6:51 am

(Apr 17, 2023 06:30 PM)php Wrote: [\[CITE\]](#) Looking forward to reading about how this Oday specifically works.

Waiting for a video showing cause all these info too much for a non related person ?

Mr. Robot - April 20, 2023, 10:00 pm

(Apr 19, 2023 06:51 AM)Be?? Wrote: [\[CITE\]](#) Waiting for a video showing cause all these info too much for a non related person ?

I've updated my thread with the best explanation I can give.