A Scanner DRACly

A PenTest Story

Vlad Grigorescu
2021-06-10

CPPC

About Me

- Security Engineer @ UIUC, CMU, NCSA, ESnet
- Core Zeek Developer
- Consultant, focused on PenTesting
- A few CVEs, a few CTF wins

What this Talk Is

- The story of a PenTest
- What defenses were in place
- How they failed (and why it matters)
- How they can be improved
- How you can build up red-team expertise

What this Talk is NOT

- A vendor pitch
- A reflection of anyone else's views
- Revolutionary

PenTest Overview: Mission

- Collaboration with a hospital on medical research
- Scope was expanded with the school's COVID response
- **Can an attacker access PHI?**

Logistics

- Determine scope
- Client provided list of subnets and access to some Slack channels
- I told the CSO when the test began and ended
- External test: No access provided
- Internal test: Virtual machine with no special access provided

Open-Source Intelligence

- Reverse DNS (`nmap -sL`)
- Certificate Transparency Logs

OSINT: EDU

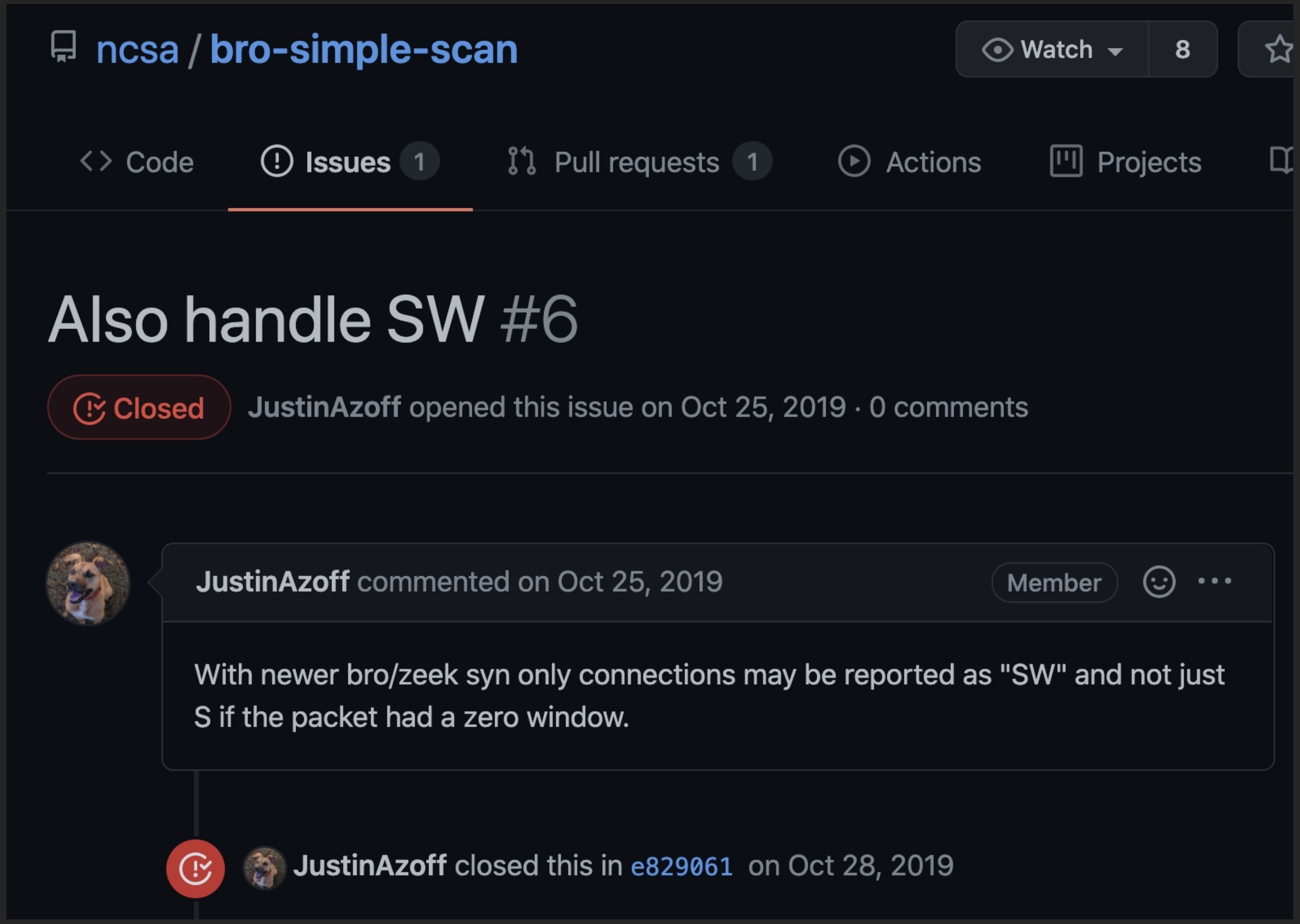
OSINT: EDU

- Mailing lists

> *We monitor two full /16, 3 /24, and 2 partial /16, in front of any local FW devices.*
>
> …
>
> *I switched to the bro-simple-scan package.*

Scanning

- bro-simple-scan



Also handle SW #6

Closed JustinAzoff opened this issue on Oct 25, 2019 · 0 comments

JustinAzoff commented on Oct 25, 2019

With newer bro/zeek syn only connections may be reported as "SW" and not just S if the packet had a zero window.

JustinAzoff closed this in e829061 on Oct 28, 2019

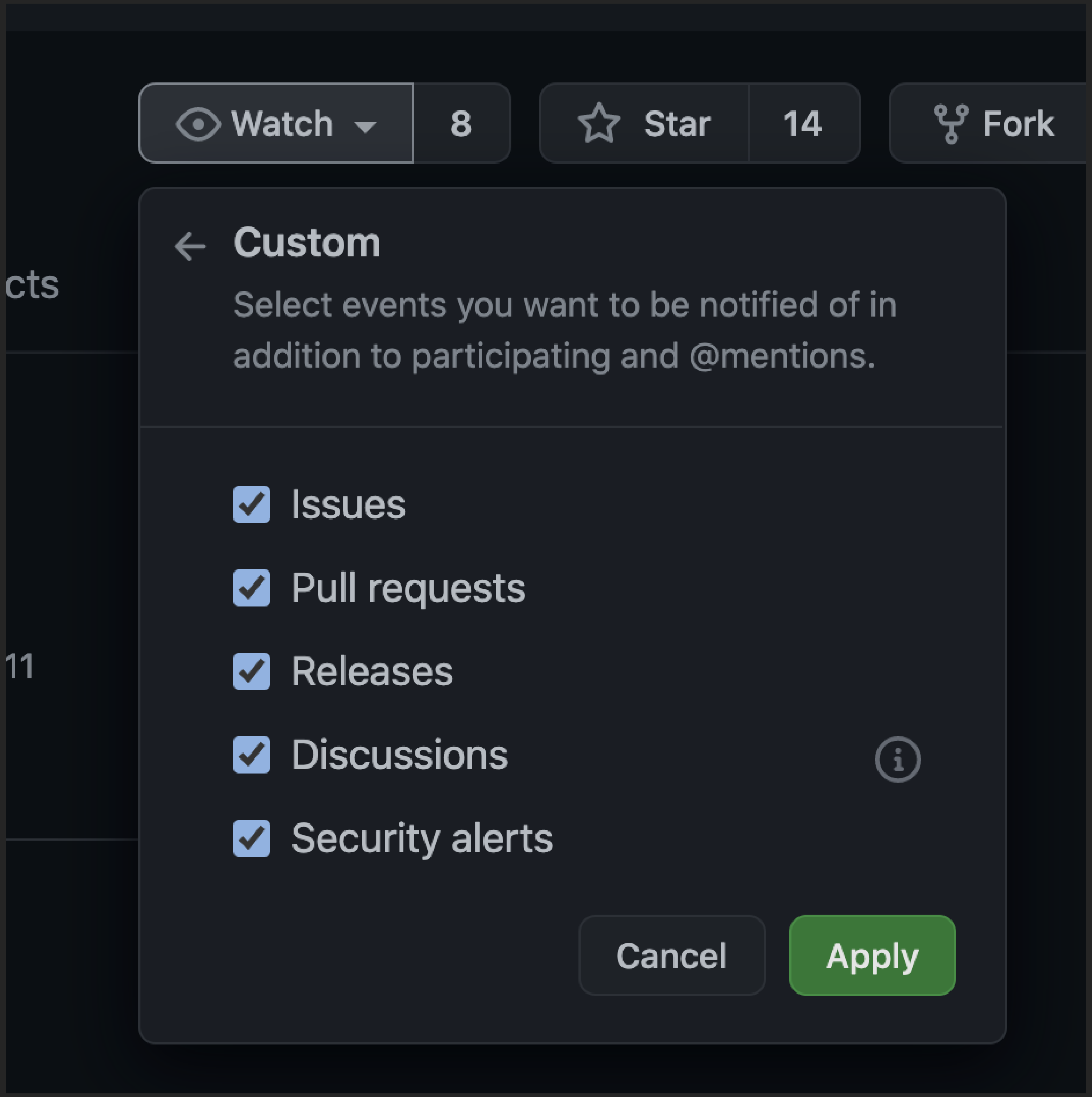
bro-simple-scan

```
  event connection_attempt(c: connection)
  {
- if ( c$history == "S" )
+ if ( c$history == "S" || c$history == "SW")
 add_scan(c$id);
  }
```

masscan

```
     static unsigned char default_tcp_template[] =
     // ...
-         "\x04\x0"     /* window fixed to 1024 */
+         "\x00\x0"     /* 0-sized window */
```

Update Zeek Packages



Custom

Select events you want to be notified of in addition to participating and @mentions.

- ☑ Issues
- ☑ Pull requests
- ☑ Releases
- ☑ Discussions
- ☑ Security alerts

Zeek ssh/main.zeek

```
event ssh_auth_attempted(c: connection, authenticated: bool)

# ...

# We can't accurately tell for compressed streams

if ( c$ssh?$compression_alg && \
     ( c$ssh$compression_alg in compression_algorithms ) )
   return;
```

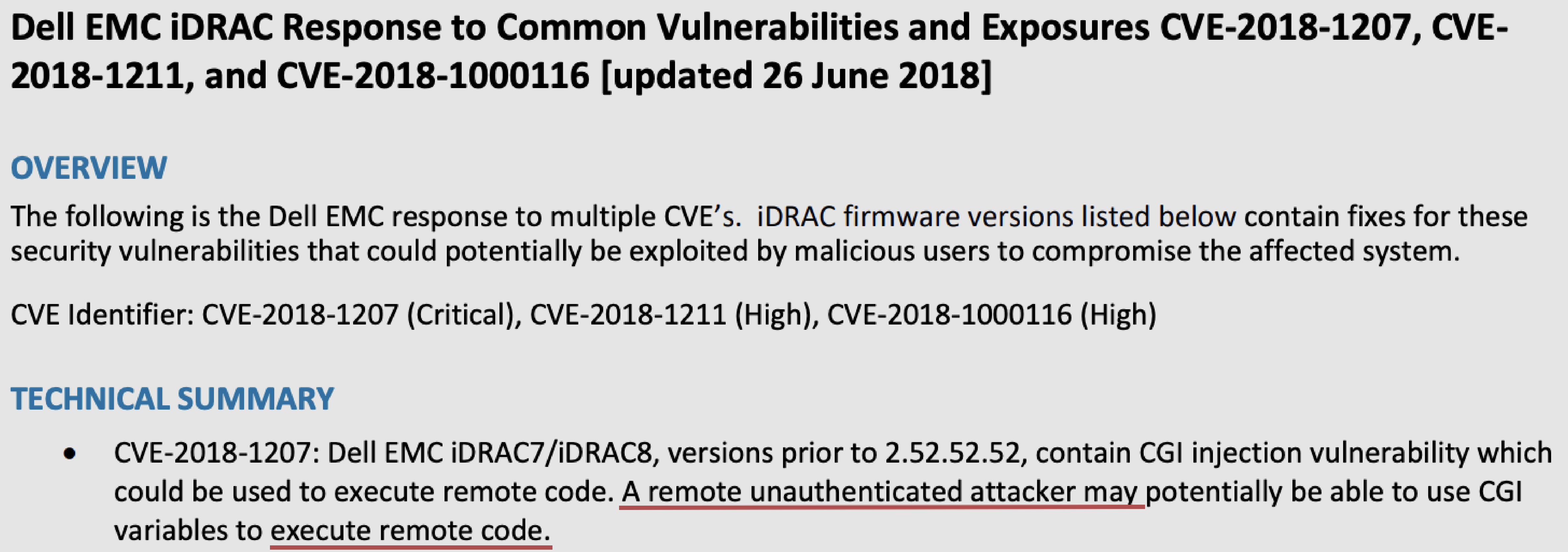
Scanning Demo

```
$ sudo masscan --ping -iL all_ips --rate 1500000 -oL -
```

Next Steps

- Look at TLS certificates
- Identify:
  - applications,
  - versions,
  - vulnerabilities

CVE-2018-1207



Dell EMC iDRAC Response to Common Vulnerabilities and Exposures CVE-2018-1207, CVE-2018-1211, and CVE-2018-1000116 [updated 26 June 2018]

OVERVIEW

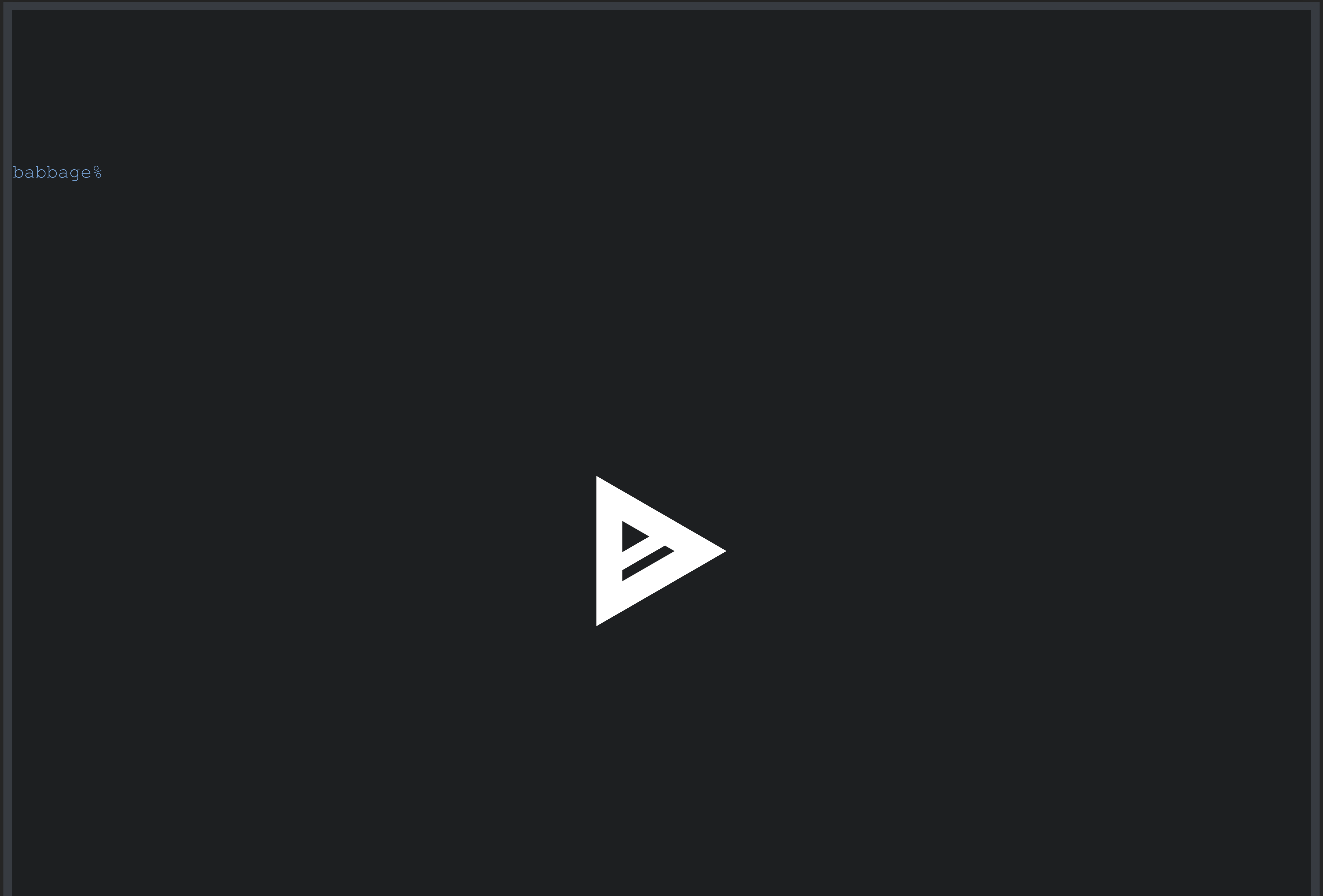
The following is the Dell EMC response to multiple CVE's. iDRAC firmware versions listed below contain fixes for these security vulnerabilities that could potentially be exploited by malicious users to compromise the affected system.

CVE Identifier: CVE-2018-1207 (Critical), CVE-2018-1211 (High), CVE-2018-1000116 (High)

TECHNICAL SUMMARY

- CVE-2018-1207: Dell EMC iDRAC7/iDRAC8, versions prior to 2.52.52.52, contain CGI injection vulnerability which could be used to execute remote code. A remote unauthenticated attacker may potentially be able to use CGI variables to execute remote code.

RCE Demo



```
babbage%
```

CVE Results