Stored XSS in MITRE CALDERA Debrief Plugin - Gist Contact

High l50 published GHSA-7344-4pg9-qf45 on Sep 22

Package

CALDERA (MITRE)

Affected versions	Patched versions
< CALDERA v4.0.0	CALDERA v4.1.0

DEBRIEF (MITRE)

< commit 7ea5d726538a27bdc33613b1c23d822f73935c6f	commit d815b603cbc639e9de509ca1331446cb3bb075aa

Description

Vulnerability Description:

A third stored cross-site scripting (XSS) vulnerability was discovered in the gist contact configuration field of MITRE CALDERA. We confirmed it was possible as the `blue` user to attack the `red` user provided through the Docker Compose CALDERA deployment. More specifically, we were able to introduce an attack as the `blue` user that resulted in the `red` user (once they triggered the vuln) to execute arbitrary commands on agents that are part of an operation.

Successful exploitation of this vulnerability can provide an attacker with the means to escalate their privileges within the application and the ability to run arbitrary code on any enrolled systems.

The vulnerability was tested on mitre/caldera@ `a1f6a91` .

Proof of Concept:

1. Create a Caldera test environment
2. Login to Caldera with the red user

3. Click Configuration
4. Set app.contact.gist to `"><img src=x onerror=prompt(document.domain)>`
5. Click **Update**
6. Click **debrief**
7. Move your mouse over the C2 Server icon
8. Observe prompt

Fix:

Remediation strategy provided by Jonathan (Jay) Yee from the MITRE Caldera development team:

This specific vulnerability in debrief was patched in mitre/debrief@ `d815b60`

The debrief plugin commit was also pinned to the latest release, caldera v4.1.0

Users running caldera versions older than v4.1.0 are urged to update the `debrief` plugin to the latest version:

```
git submodule update --remote --force plugins/debrief
```

Patched plugin: Patched commit

Timeline:

Reported: September 19th, 2022
Acknowledged: September 21st, 2022
Fixed: September 21st, 2022

Severity

High

CVE ID

CVE-2022-41139

Weaknesses

CWE-20 CWE-79

Credits


I50