

New issue

Jump to bottom

# Open redirect vulnerability in CommonController.ClearCache method #2113

Closed eric-therond-sonarsource opened this issue on Oct 8, 2020 · 1 comment

Assignees



Labels

review security

Milestone

4.1

eric-therond-son... commented on Oct 8, 2020

Hello  
This issue to address this open redirect vulnerability in the `CommonController.ClearCache` method.

Example:

Request

Raw Params Headers Hex

1 GET /backend/admin/common/clearcache?previousUrl=https://www.google.fr HTTP/1.1  
2  
3  
4

Response

Raw Headers Hex

1 HTTP/1.1 302 Found  
2 Cache-Control: private  
3 Content-Type: text/html; charset=utf-8  
4 Location: https://www.google.fr  
5 Server: Microsoft-IIS/10.0  
6 X-AspNetMvc-Version: 5.2  
7 X-AspNet-Version: 4.0.30319  
8 X-Powered-By: ASP.NET  
9 Date: Thu, 08 Oct 2020 15:00:44 GMT  
10 Connection: close  
11 Content-Length: 138  
12  
13 <html>  
14 <head>  
15 <title>  
16 Object moved  
17 </title>  
18 </head>  
19 <body>  
20 Object moved to <a href="https://www.google.fr">here</a>  
21

Eric

eric-therond-son... commented on Oct 8, 2020 • edited

Author

The same vulnerability exists in the:

- `ClearDatabaseCache` method
- `RestartApplication` method
- `ScheduleTaskController.Edit` method

muratcakir assigned mgesing on Oct 8, 2020

muratcakir added review security labels on Oct 8, 2020

muratcakir added this to the 4.1 milestone on Oct 8, 2020

mgesing closed this as completed in 648a527 on Oct 13, 2020

eric-therond-sonarsource mentioned this issue on Oct 13, 2020

Path Traversal Vulnerability #2112

Closed

Akokonunes mentioned this issue on Feb 1

Create CVE-2020-36365.yaml projectdiscovery/nuclei-templates#3650

Merged

Assignees

mgesing

Labels

review security

Projects

None yet

Milestone

---

Development  
No branches or pull requests

---

3 participants

