Advisory ID: usd-2021-0008
CVE Number: CVE-2021-21990
Affected Product: VMware Workspace
Vulnerability Type: CWE-79: Cross-site
Security Risk: Low
Vendor URL: https://www.vmware.com
Vendor Status: Fixed

Description

A VMware endpoint reflects user controlled contents without sanitization, resulting in limited reflected Cross-Site Scripting. The endpoint reflects the Referer HTTP header contents within an HTTP redirect's Location header without any sanitization. As it allows arbitrary domains, this enables an Open Redirect vulnerability. Further, as arbitrary schemes are allowed, using a data-URI as Referer leads to JavaScript execution in a victim's browser and under certain circumstances.

Cross-Site Scripting vulnerabilities could arise if user controlled contents are reflected without sufficient and context-aware sanitization and/or encoding. If a malicious actor is able to inject malicious JavaScript which is run within the context of an application and in a victim's browser and session, the malicious actor could potentially steal sensitive information or perform actions on behalf of the victim.

Proof of Concept (PoC)

The following request response pairs illustrate how the vulnerability could be exploited.

Please note that we redacted the exact subdomain of awmdm.com – our tests were performed against a generic AirWatch Hosted (SaaS) instance.

1. Open Redirect

Request:

```
GET /DeviceManagement/Enrollment/IsMamEnrollmentEnabled?groupId=%3ca HTTP/1.1
Host: abcdef.awmdm.com
Referer: https://www.usd.de/
```

Response:

```
HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: https://www.usd.de/
[…]
<h2>Object moved to <a href="https://www.usd.de/">here</a>.</h2>
```

2. Limited XSS

Request:

```
GET /DeviceManagement/Enrollment/IsMamEnrollmentEnabled?groupId=%3ca HTTP/1.1
Host: abcdef.awmdm.com
Referer: data:text/html,alert(1)
```

Response:

```
HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: data:text/html,%3Cscript%3Ealert(1)%3C/script%3E
[…]
<h2>Object moved to <a>here</a>.</h2>
```

Safari on iOS renders HTML and evalu ader:

Fix

It is recommended to consider all user input to the application as potentially malicious. All input to the application should be verified and if necessary replaced. Meta characters should be treated with care. The majority of programming languages supports standard procedures for filtering and replacing meta characters. For example, PHP has the built-in function *htmlspecialchars()*. It is recommended to use whitelisting wherever possible.

Timeline

- 2021-03-12: This vulnerability was identified by Leif Enders and Lauritz Holtmann.
- 2021-03-14: Advisory submitted to vendor via e-mail.
- 2021-04-08: Vendor informs about upcoming fix.
- 2021-05-11: Advisory for CVE-2021-21990 is released by VMware: https://www.vmware.com/security/advisories/VMSA-2021-0008.html
- 2021-05-31: Security advisory released by usd AG.

Credits

This security vulnerability was found by Leif Enders and Lauritz Holtmann of usd AG.

About usd Security Advisories

In order to protect businesses against hackers and criminals, we always have to keep our skills and knowledge up to date. Thus, security research is just as important for our work as is building up a security community to promote the exchange of knowledge. After all, more security can only be achieved if many individuals take on the task.

Our CST Academy and our usd HeroLab are essential parts of our security mission. We share the knowledge we gain in our practical work and our research through training courses and publications. In this context, the usd HeroLab publishes a series of papers on new vulnerabilities and current security issues.

Always for the sake of our mission: „more security."

to usd AG

In accordance with usd AG's Responsible Disclosure Policy, all vendors have been notified of the existence of these vulnerabilities.

Disclaimer

The information provided in this securi ecurity advisory may be updated in order to provide as accurate informati

Security Advisory zu GitLab

Dez 15, 2022

Security Advisory zu Acronis Cyber

Nov 9, 2022

Security Advisories zu Apache Tomcat

Nov 24, 2022