XSS in Rustici Software SCORM Engine

Medium

← View More Research Advisories

Synopsis

Tenable discovered a cross-site scripting (XSS) vulnerability in the **playerConfUrl** parameter of the Scorm/Rustici Engine interface **/defaultui/player/modern.html** page. This XSS vulnerability could be leveraged by an attacker to achieve full account takeover against cloud.scorm.com users, and could affect any other LMS which integrates this page, with varying impact.

The issue appears to occur as a result of the call to **loadCode(playerConfigurationurl,false)** in **/defaultui/src/js/integration/loader.js**, as **playerConfigurationUrl** is user-defined and has no limitations in terms of what domain it loads code from, or what kind of URI it accepts. As a result an attacker could craft a malicious link which loads a malicious javascript file from an external site, or uses a **data:** uri to pass javascript directly.

Proof of Concept:

As Rustici has fixed these issues, the following proof of concept

```
https://[app-using-scorm]/[path-to-scorm-files]/defaultui/player/modern.html?
playerConfUrl=data:text,alert(document.domain)//
```

Solution

Update to SCORM engine 20.1.45.914+ or 21.1.7.219+

Additional References

https://support.scorm.com/hc/en-us/articles/6191663599259-Engine-and-Engine-Dispatch-20-1-45-914

9 March, 2022 - Tenable requests a security contact for Rustici Software
9 March, 2022 - Rustici responds, indicating the issue can be reported to support
10 March, 2022 - Tenable reports the issue details to Rustici
10 March, 2022 - Rustici confirms the issue
6 April, 2022 - Rustici informs Tenable that the issue had been fixed in 21.1.7.219, released prior to Tenable's report.
6 April, 2022 - Rustici indicates they are still working on upgrading SCORM Cloud and addressing the issue for versions < v21
6 June, 2022 - Tenable notices that the issue appears to have been fixed in SCORM Cloud, requests an update, reminds Rustici of June 8th 90-day disclosure date
6 June, 2022 - Rustici confirms that SCORM Cloud has been upgraded to the latest engine version, and that the fix has been backported to Engine 20.1.
6 June, 2022 - Rustici requests that more time be allowed before disclosure, for other LMS who integrate SCORM into their product to upgrade versions
7 June, 2022 - Tenable informs Rustici that the 90-day disclosure date is final and that an advisory will be published on June 8th.

Tenable takes product security very seriously. If you believe you have found a vulnerability in one of our products, we ask that you please work with us to quickly resolve it in order to protect customers. Tenable believes in responding quickly to such reports, maintaining communication with researchers, and providing a solution in short order.

For more details on submitting vulnerability information, please see our Vulnerability Reporting Guidelines page.

If you have questions or corrections about this advisory, please email advisories@tenable.com

Risk Information

CVE ID: CVE-2022-2035
Tenable Advisory ID: TRA-2022-21
Credit: Evan Grant
CVSSv3 Base / Temporal Score: 6.1
CVSSv3 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Affected Products: SCORM Engine 21.1.x < 21.1.7.219
SCORM Engine < 20.1.45.914

8 June 2022 – Advisory published

FEATURED PRODUCTS

Tenable One Exposure Management Platform

Tenable.cs Cloud Security

Tenable.io Vulnerability Management

Tenable.io Web App Scanning

Tenable.asm External Attack Surface

Tenable.ad Active Directory

Tenable.ot Operational Technology

Tenable.sc Security Center

Tenable Lumin

Nessus

→ View all Products

FEATURED SOLUTIONS

Application Security

Building Management Systems

Cloud Security

Compliance

Exposure Management

Finance

Healthcare