

Vulnerability Advisory

Name	www.smule.com Multiple Cross Site Scripting
Vendor Advisory	Nil
Date Released	13 January 2010
Affected Software	www.smule.com and all subdomains
Researcher	CodeScan Labs (advisories@codescan.com)

Description

CodeScan Labs has been informed by an external third party of multiple vulnerabilities in the website smule.com. This information has identified a number of potential issues which warrant further investigation.

Based on the severity of the vulnerabilities identified, action should be taken as soon as possible to prevent any potential risk to users of smule.com.

Multiple attempts have been made to contact smule.com regarding these issues.

Vulnerability

A number of Reflected Cross-Site Scripting (XSS) have been identified in the publically accessible portions of smule.com. Reflected Cross-Site Scripting vulnerabilities occur when user input is not sufficiently sanitized before it is returned to the user.

1. The search engine that is accessible across all subdomains of smule.com does not sufficiently sanitize user input passed through the GET request. All data entered in either via the search box or manual manipulation of the URL can be manipulated to determine the vulnerability to XSS.
2. The Ocarina Score Generator does not sufficiently sanitize any of the Query String parameters for malicious input. This gives multiple potential XSS paths to a malicious user.

A malicious user could craft a URL which modifies the page content on-the-fly to steal login credentials and personal information. By giving this URL to unsuspecting users, they will believe (and rightly so) that they are dealing with smule.com, as the page content is displayed within their domain. However the malicious user can log this information, and use it for their own benefit.

These URLs could also be used to serve malware to unsuspecting users, once again playing on their trust of smule.com. By placing downloads within the page content through a specially crafted URL, and then giving this link to unsuspecting users, they could be fooled into downloading unwanted and malicious software under the guise of being from smule.com.

Solution

Smule users should be careful in determining whether smule links are safe, and take care against standard phishing attacks based around the reported issues.

About CodeScan Labs

CodeScan Labs is the worlds leading provider of Web Source Code vulnerability assessment and remediation tools. CodeScan™ rates and identifies the strength of your web applications within your network.

CodeScan Labs is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products where possible. Members of the CodeScan Labs R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

For further information on this issue or any of our service offerings, contact us

Web www.codescan.com
Email info@codescan.com
Phone +649 309 7650