SecureAuth security advisory - AngularJS client-side template injection

Released: June 15, 2020

Last Updated: July 1, 2020

Summary

The SecureAuth® Identity Platform (formerly SecureAuth IdP) uses AngularJS for rendering pages within its Themes environment. Improper sanitization on the characters “{{“ and “}}” can result in an exploitation of the AngularJS components.

Within the Identity Platform, the username field could be manipulated to exploit this vulnerability if a malicious administrator created a username with the appropriate payload in the username and trick an end user into utilizing the modified username.

Criticality

CVSS3.1 Score	2.0
Criticality	LOW
Vector String	CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:N

Description

All versions of AngularJS are susceptible to client-side template injection by utilizing a payload enclosed in “{{“ and “}}”. An attacker could execute cross-site scripting against a user through this method which could potentially expose information such as cookies or other browser information, which could then be used to further access information or services.

Within the Identity Platform, AngularJS is used in the Themes module to render login pages to unauthenticated users. These forms did perform input sanitization and validation on the server side; however, the “{{“ and “}}” were not included in previous version of the Themes module. The hotfix related to this vulnerability includes server-side input sanitization and validation for the characters used to exploit this issue.

This attack appears to be only possible if a malicious administrator created or modified a user to include attack code within the username registered in the directory store configured for the Identity Platform. For example, a susceptible username would be “user123{{constructor.constructor('alert(1)')()}}” and the malicious administrator would need to convince the end user that this username is their valid username to authentication via the Identity Platform.

Impact

The attacker could initiate a cross-site scripting attack against a user to potentially steal browser information such as authentication cookies.

Affected Products

All supported Identity Platform/SecureAuth IdP products (9.1, 9.2, 9.3, and 19.07) running on any version of Windows Server are vulnerable to this issue.

Workaround and Solution

Workaround

Identity Platform administrators can potentially minimize the impact of this vulnerability by performing the following:

- Ensure the X-XSS-Protection header within the Internet Information Server (IIS) is set to “1; mode=block” to enable the cross-site scripting protections in users’ browsers when visiting an Identity Platform login page.
- Implement monitoring and alerting of new users within the directory store used for authentication to watch for new or modified users with “{{“ and /or “}}” contained in the username.

Solution

Identity Platform/SecureAuth IdP version	Hotfix number
9.1	9.1.0-57
9.2	9.2.0-34

9.3	9.3.0-17
19.07	19.07-3
19.07.01	19.07.01-11

Please contact SecureAuth Customer Support (support@secureauth.com) to assist in implementing the patch for the appropriate realms with the Identity Platform.

References

Vulnerability References

- https://portswigger.net/research/xss-without-html-client-side-template-injection-with-angularjs
- CVSS3.1 Scoring Calculator: https://www.first.org/cvss/calculator/3.1
- CVSS3.1 Guide: https://www.first.org/cvss/v3.1/user-guide

SecureAuth Product Security Public Polices

- Vulnerability Disclosure Policy: https://www.secureauth.com/vulnerability-disclosure-policy
- Product End of Life Policy: https://support.secureauth.com/hc/en-us/articles/360019889171-Support-Lifecycle-Policy-and-End-of-Life-Dates

Acknowledgement and Credit

SecureAuth would like to thank Bishop Fox for notifying us about this vulnerability.

Revision History

Version	Date	Author	Comments
1.0	June 15, 2020	SecureAuth PSIRT	Initial release
1.1	July 1, 2020	SecureAuth PSIRT	Updated hotfixes for all versions