GUI/AXAPI - VULNERABILITIES #1 - ACOS 3.X, 4.X

PUBLISHED: AUGUST 4, 2017 | LAST UPDATE: APRIL 5, 2018

SUMMARY

Web application security and vulnerability scans of the ACOS management interface indicated a range of security weaknesses and exposures to potential attacks in the ACOS 3.x and 4.x GUI and AXAPI services. Accordingly, the following vulnerabilities are addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	http-generic-click-jacking	Rapid7	4 Severe	Click Jacking [1]
2	(a)	OWASP	Low	Strict-Transport-Security Header Not Set [2]
3	(a)	OWASP	Low	Incomplete or No Cache-control and Pragma HTTP Header Set [3]
4	(a)	OWASP	Low	Web Browser XSS Protection Not Enabled [4]
5	(a)	OWASP	Low	X-Content-Type-Options Header Missing [5]
6	(a)	OWASP	Low	Content Security Policy (CSP) Header Not Set [6]
7	(a)	OWASP	Informational	Storable and Cacheable Content [7]
8	(a)	OWASP	Medium	X-Frame-Options Header Not Set [8]
9	http-cookie-secure-flag	Rapid7	5 Severe	Missing Secure Flag From SSL Cookie [9]
10	http-cookie-http-only-flag	Rapid7	5 Severe	Missing HttpOnly Flag From Cookie [10]
11	(a)	OWASP	Medium	Buffer Overflow [11]
12	(a)	OWASP	Low	Cookie No HttpOnly Flag [12]
13	(a)	OWASP	Low	Cookie Without Secure Flag [13]
14	(a)	OWASP	Low	Cookie Without SameSite Attribute [14]

(a) No identifier available. See item Summary.

AFFECTED RELEASES

The table below indicates releases of ACOS exposed to these vulnerabilities and ACOS releases that address these issues or are otherwise unaffected by them.

Customers using affected ACOS releases can overcome vulnerability exposures by updating to the indicated resolved release. If the table does not list a corresponding resolved or unaffected release, then no ACOS release update is currently available.

Releases Affected			Releases Resolved or Unaffected
4.1.2			4.1.2-P1
4.1.1	–	4.1.1-P2	4.1.1-P3
4.1.0	–	4.1.0-P9	4.1.0-P10
3.1.0-P1	–	3.2.1-P1	3.2.2-P1 (a), 3.2.2-P3 (b)
3.2.2-P1	–	3.2.2-P2	3.2.2-P3 (b)

(a) Addresses items 1 – 8 listed above.

(b) Addresses items 9 – 14 listed above.

WORKAROUNDS AND MITIGATIONS

Common security best practices in the industry for network appliance management and control planes can enhance protection against remote malicious attacks. Limit the exploitable attack surface for critical, infrastructure, networking equipment through the use of access lists or firewall filters to and from only trusted, administrative networks or hosts.

SOFTWARE UPDATES

Software updates that address these vulnerabilities are or will be published at the following URL:

http://www.a10networks.com/support/axseries/software-downloads

VULNERABILITY DETAILS

The following table shares brief descriptions for the vulnerabilities addressed in this document.

Vulnerability ID	Description
http-generic-click-jacking	Clickjacking, also known as a UI redress attack, is a method in which an attacker uses multiple transparent or opaque layers to trick a user into clicking a button or link on a page other than the one they believe they are clicking. Thus, the attacker is "hijacking" clicks meant for one page and routing the user to an illegitimate page.
Strict-Transport-Security Header Not Set	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Incomplete or No Cache-control and Pragma HTTP Header Set	The cache-control and pragma HTTP header have not been set properly or are missing allowing the browser and proxies to cache content.
Web Browser XSS Protection Not Enabled	Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'.
X-Content-Type-Options Header Missing	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
Content Security Policy (CSP) Header Not Set	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Storable and Cacheable Content	The response contents are storable by caching components such as proxy servers, and may be retrieved directly from the cache, rather than from the origin server by the caching servers, in response to similar requests from other users. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where "shared" caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
X-Frame-Options Header Not Set	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
http-cookie-secure-flag	The Secure attribute tells the browser to only send the cookie if the request is being sent over a secure channel such as HTTPS. This will help protect the cookie from being passed over unencrypted requests. If the

	application can be accessed over both HTTP and HTTPS, then there is the potential that the cookie can be sent in clear text.
http-cookie-http-only-flag	HttpOnly is an additional flag included in a Set-Cookie HTTP response header. If supported by the browser, using the HttpOnly flag when generating a cookie helps mitigate the risk of client side script accessing the protected cookie. If a browser that supports HttpOnly detects a cookie containing the HttpOnly flag, and client side script code attempts to read the cookie, the browser returns an empty string as the result. This causes the attack to fail by preventing the malicious (usually XSS) code from sending the data to an attacker's website.
Buffer Overflow	Buffer overflow errors are characterized by the overwriting of memory spaces of the background web process, which should have never been modified intentionally or unintentionally. Overwriting values of the IP (Instruction Pointer), BP (Base Pointer) and other registers causes exceptions, segmentation faults, and other process errors to occur. Usually these errors end execution of the application in an unexpected way.
Cookie No HttpOnly Flag	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Cookie Without Secure Flag	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Cookie Without SameSite Attribute	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

RELATED LINKS

Ref #	General Link
[1]	Rapid7: Click Jacking
[2]	OWASP: HTTP Strict Transport Security
[3]	OWASP: Session Management Cheat Sheet - Web Content Caching
[4]	OWASP: XSS (Cross Site Scripting) Prevention Cheat Sheet
[5]	OWASP_List of useful HTTP headers, MSDN: Reducing MIME type security risks
[6]	OWASP: Content Security Policy
[7]	IETF: RFC-7234 -HTTP 1.1: Caching, RFC-7231 - Semantics and Content
[8]	MSDN: Combating ClickJacking With X-Frame-Options
[9]	Rapid7: Missing Secure Flag From SSL Cookie
[10]	Rapid7: Missing HttpOnly Flag From Cookie
[11]	OWASP: Buffer overflow attack
[12]	OWASP: HttpOnly
[13]	OWASP: Testing for cookies attributes (OTG-SESS-002)
[14]	IETF: draft-ietf-httpbis-cookie-same-site-00 - Same-Site Cookies

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2017-08-04	Initial Publication
2.0	2018-03-07	Update release information for ACOS 4.1.0 and 3.2.2 release families. Corrected affected releases for ACOS 4.1.0.
3.0	2018-04-05	Added ACOS 3.2.2 affected and resolved release information