acunetix

Developer Report

Acunetix Security Audit

19 June 2018

Generated by Acunetix

Scan of https://nxtstep.eastus.cloudapp.azure.com/mlrefarch/

Scan details

Scan information	
Start time	19/06/2018, 17:05:52
Start url	https://nxtstep.eastus.cloudapp.azure.com/mlrefarch/
Host	https://nxtstep.eastus.cloudapp.azure.com/mlrefarch/
Scan time	1 minutes, 26 seconds
Profile	Full Scan

Threat level

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution

Total alerts found	2
High	0
Medium	1
Low	1
Informational	0

Alerts summary

Insecure crossdomain.xml file

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 6.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CWE	CWE-284

Affected items	Variation
Web Server	1

Clickjacking: X-Frame-Options header missing

Classification	
CVSS2	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-693

Affected items	Variation
Web Server	1

Alerts details

Insecure crossdomain.xml file

Severity	**Medium**
Reported by module	/Scripts/PerServer/Crossdomain_XML.script

Description

The browser security model normally prevents web content from one domain from accessing data from another domain. This is commonly known as the "same origin policy". URL policy files grant cross-domain permissions for reading data. They permit operations that are not permitted by default. The URL policy file is located, by default, in the root directory of the target server, with the name crossdomain.xml (for example, at www.example.com/crossdomain.xml).

When a domain is specified in crossdomain.xml file, the site declares that it is willing to allow the operators of any servers in that domain to obtain any document on the server where the policy file resides. The crossdomain.xml file deployed on this website opens the server to all domains (use of a single asterisk "*" as a pure wildcard is supported) like so:

```
<cross-domain-policy>

<allow-access-from domain="*" />

</cross-domain-policy>
```

This practice is suitable for public servers, but should not be used for sites located behind a firewall because it could permit access to protected areas. It should not be used for sites that require authentication in the form of passwords or cookies. Sites that use the common practice of authentication based on cookies to access private or user-specific data should be especially careful when using cross-domain policy files.

Impact

Using an insecure cross-domain policy file could expose your site to various attacks.

Recommendation

Carefully evaluate which sites will be allowed to make cross-domain calls. Consider network topology and any authentication mechanisms that will be affected by the configuration or implementation of the cross-domain policy.

References

Cross-domain policy file usage recommendations for Flash Player (http://www.adobe.com/devnet/flashplayer/articles/cross_domain_policy.html)
Cross-domain policy files (http://blogs.adobe.com/stateofsecurity/2007/07/crossdomain_policy_files_1.html)

Affected items

Web Server
Details
The crossdomain.xml file is located at **/crossdomain.xml**.
Request headers

```
GET /crossdomain.xml HTTP/1.1
Accept: */*
Accept-Encoding: gzip,deflate
Host: nxtstep.eastus.cloudapp.azure.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Proxy-Connection: keep-alive
```

Clickjacking: X-Frame-Options header missing

Severity	**Low**
Reported by module	/Scripts/PerServer/Clickjacking_X_Frame_Options.script

Description

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server didn't return an **X-Frame-Options** header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

Impact

The impact depends on the affected web application.

Recommendation

Configure your web server to include an X-Frame-Options header. Consult Web references for more information about the possible values for this header.

References

The X-Frame-Options response header (https://developer.mozilla.org/en-US/docs/HTTP/X-Frame-Options)
Clickjacking (http://en.wikipedia.org/wiki/Clickjacking)
OWASP Clickjacking (https://www.owasp.org/index.php/Clickjacking)
Defending with Content Security Policy frame-ancestors directive (https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet#Defending_with_Content_Security_Policy_frame-ancestors_directive)
Frame Buster Buster (http://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed)

Affected items

Web Server

Details

Request headers

```
GET / HTTP/1.1
Accept: */*
Accept-Encoding: gzip,deflate
Host: nxtstep.eastus.cloudapp.azure.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Proxy-Connection: keep-alive
```

Scanned items (coverage report)

https://nxtstep.eastus.cloudapp.azure.com/
https://nxtstep.eastus.cloudapp.azure.com/mlrefarch
https://nxtstep.eastus.cloudapp.azure.com/mlrefarch/css
https://nxtstep.eastus.cloudapp.azure.com/mlrefarch/css.css
https://nxtstep.eastus.cloudapp.azure.com/mlrefarch/css/menustyle.css
https://nxtstep.eastus.cloudapp.azure.com/mlrefarch/css/styles.css
https://nxtstep.eastus.cloudapp.azure.com/mlrefarch/css/verticalmenustyles.css
https://nxtstep.eastus.cloudapp.azure.com/mlrefarch/icon
https://nxtstep.eastus.cloudapp.azure.com/mlrefarch/images
https://nxtstep.eastus.cloudapp.azure.com/mlrefarch/js
https://nxtstep.eastus.cloudapp.azure.com/mlrefarch/js/jquery-1.11.0.min.js
https://nxtstep.eastus.cloudapp.azure.com/mlrefarch/js/ReferenceImplementationForML.js
https://nxtstep.eastus.cloudapp.azure.com/mlrefarch/js/verticalmenuscript.js