acunetix

Developer Report

Acunetix Security Audit

19 June 2018

Generated by Acunetix

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

Scan details

Scan information	
Start time	19/06/2018, 17:01:09
Start url	https://nxtstep.eastus.cloudapp.azure.com/accelerator/
Host	https://nxtstep.eastus.cloudapp.azure.com/accelerator/
Scan time	2 minutes, 5 seconds
Profile	Full Scan

Threat level

Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

Alerts distribution

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

Alerts summary

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

Insecure response with wildcard '*' in Access-Control-Allow-Origin

Classification	
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None 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
CWE	CWE-16

Affected items	Variation
/accelerator	1

Alerts details

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
```

Insecure response with wildcard '*' in Access-Control-Allow-Origin

Severity	**Low**
Reported by module	/Scripts/PerFolder/Access_Control_Allow_Origin_Dir.script

Description

Cross-origin resource sharing (CORS) is a mechanism that allows restricted resources (e.g. fonts) on a web page to be requested from another domain outside the domain from which the resource originated. The Access-Control-Allow-Origin header indicates whether a resource can be shared based by returning the value of the Origin request header, "*", or "null" in the

response.

If a website responds with Access-Control-Allow-Origin: * the requested resource allows sharing with every origin. Therefore, any website can make XHR (XMLHTTPRequest) requests to your site and access the responses. It's not recommended to use the Access-Control-Allow-Origin: * header.

Impact

Any website can make XHR requests to your site and access the responses.

Recommendation

Is recommended not to use Access-Control-Allow-Origin: *. Instead the Access-Control-Allow-Origin header should contain the list of origins that can make COR requests.

References

Test Cross Origin Resource Sharing (OTG-CLIENT-007) (https://www.owasp.org/index.php/Test_Cross_Origin_Resource_Sharing_(OTG-CLIENT-007))
Cross-origin resource sharing (https://en.wikipedia.org/wiki/Cross-origin_resource_sharing)
Cross-Origin Resource Sharing (http://www.w3.org/TR/cors/)
CrossOriginRequestSecurity (https://code.google.com/p/html5security/wiki/CrossOriginRequestSecurity)

Affected items

/accelerator

Details

Request headers

```
GET /accelerator/ 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/accelerator
https://nxtstep.eastus.cloudapp.azure.com/accelerator/assets
https://nxtstep.eastus.cloudapp.azure.com/accelerator/assets/css
https://nxtstep.eastus.cloudapp.azure.com/accelerator/assets/css/bootstrap-grid.min.css
https://nxtstep.eastus.cloudapp.azure.com/accelerator/assets/css/bootstrap.min.css
https://nxtstep.eastus.cloudapp.azure.com/accelerator/assets/css/indigo-pink.css
https://nxtstep.eastus.cloudapp.azure.com/accelerator/inline.917526ff957f5e55abac.bundle.js
https://nxtstep.eastus.cloudapp.azure.com/accelerator/main.ef3f50190efec8e32613.bundle.js
https://nxtstep.eastus.cloudapp.azure.com/accelerator/polyfills.7897595c57594b4e3c69.bundle.js
https://nxtstep.eastus.cloudapp.azure.com/accelerator/styles.4033f0f710a121ed4812.bundle.css