Developer Report

Acunetix Security Audit

19 June 2018

Generated by Acunetix

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

Scan details

Scan information	
Start time	19/06/2018, 17:24:21
Start url	https://nxtstep.eastus.cloudapp.azure.com/webaccelerator/
Host	https://nxtstep.eastus.cloudapp.azure.com/webaccelerator/
Scan time	1 minutes, 23 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	1
! High	0
! Medium	0
! Low	1
i Informational	0

Alerts summary

ⓘ 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
/webaccelerator	1

Alerts details

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

/webaccelerator

Details

Request headers

```
GET /webaccelerator/ 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/webaccelerator