



# Developer Report

Acunetix Security Audit

19 June 2018

# Scan of https://nextstep.mphasis.com/crt/Dashboard.html

## Scan details





Scan information	
Start time	19/06/2018, 17:38:59
Start url	https://nextstep.mphasis.com/crt/Dashboard.html
Host	https://nextstep.mphasis.com/crt/Dashboard.html
Scan time	8 minutes, 25 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	6
 High	0
 Medium	5
 Low	1
 Informational	0

## Alerts summary

### Vulnerable Javascript library

Classification		
CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial 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-16	
Affected items		Variation
<a href="#">/crt/js/jquery-1.3.2.js</a>		1
<a href="#">/crt/js/jquery-1.4.2.js</a>		1
<a href="#">/crt/js/jquery-1.9.0.min.js</a>		1
<a href="#">/crt/js/jquery-ui-1.7.2.custom.min.js</a>		1
<a href="#">/crt/js/jquery.ui.datepicker.js</a>		1

### ASP.NET version disclosure

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	
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None	

		Availability Impact: None
CWE	CWE-200	
Affected items		Variation
<a href="#">Web Server</a>		1

## Alerts details

### Vulnerable Javascript library

Severity	Medium
Reported by module	/Scripts/PerFile/Javascript_Libraries_Audit.script

#### Description

You are using a vulnerable Javascript library. One or more vulnerabilities were reported for this version of the Javascript library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported.

#### Impact

Consult References for more information.

#### Recommendation

Upgrade to the latest version.

#### Affected items

<b>/crt/js/jquery-1.3.2.js</b>
Details
Detected Javascript library <b>jquery</b> version <b>1.3.2</b> . The version was detected from <b>filename, file content</b> .
References:
<ul style="list-style-type: none"><li>• <a href="http://bugs.jquery.com/ticket/11290">http://bugs.jquery.com/ticket/11290</a></li><li>• <a href="http://research.insecurelabs.org/jquery/test/">http://research.insecurelabs.org/jquery/test/</a></li></ul>
Request headers
GET /crt/js/jquery-1.3.2.js HTTP/1.1 Accept: */* Accept-Encoding: gzip,deflate Host: nextstep.mphasis.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 Authorization: Basic bXB0eXNpc1xzcmloYXJpLnI6NmhhZnlnhJGhyZWU=
<b>/crt/js/jquery-1.4.2.js</b>
Details
Detected Javascript library <b>jquery</b> version <b>1.4.2</b> . The version was detected from <b>filename, file content</b> .
References:
<ul style="list-style-type: none"><li>• <a href="https://github.com/jquery/jquery/issues/2432">https://github.com/jquery/jquery/issues/2432</a></li><li>• <a href="http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/">http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/</a></li></ul>
Request headers
GET /crt/js/jquery-1.4.2.js HTTP/1.1 Accept: */* Accept-Encoding: gzip,deflate Host: nextstep.mphasis.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 Authorization: Basic bXB0eXNpc1xzcmloYXJpLnI6NmhhZnlnhJGhyZWU=

/crt/js/jquery-1.9.0.min.js
<p>Details</p> <p>Detected Javascript library <b>jquery</b> version <b>1.9.0</b>. The version was detected from <b>filename, file content</b>.</p> <p>References:</p> <ul style="list-style-type: none"> <li>• <a href="https://github.com/jquery/jquery/issues/2432">https://github.com/jquery/jquery/issues/2432</a></li> <li>• <a href="http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/">http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/</a></li> </ul>
<p>Request headers</p> <pre>GET /crt/js/jquery-1.9.0.min.js HTTP/1.1 Accept: */* Accept-Encoding: gzip,deflate Host: nextstep.mphasis.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 Authorization: Basic bXB0YXNpc1xzcmloYXJpLnI6NmhhZnlnhJGhyZWU=</pre>
/crt/js/jquery-ui-1.7.2.custom.min.js
<p>Details</p> <p>Detected Javascript library <b>jquery-ui-dialog</b> version <b>1.7.2.custom</b>. The version was detected from <b>filename, file content</b>.</p> <p>References:</p> <ul style="list-style-type: none"> <li>• <a href="https://nodesecurity.io/advisories/127">https://nodesecurity.io/advisories/127</a></li> <li>• <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7103">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7103</a></li> <li>• <a href="https://www.cvedetails.com/cve/CVE-2016-7103/">https://www.cvedetails.com/cve/CVE-2016-7103/</a></li> </ul>
<p>Request headers</p> <pre>GET /crt/js/jquery-ui-1.7.2.custom.min.js HTTP/1.1 Accept: */* Accept-Encoding: gzip,deflate Host: nextstep.mphasis.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 Authorization: Basic bXB0YXNpc1xzcmloYXJpLnI6NmhhZnlnhJGhyZWU=</pre>
/crt/js/jquery.ui.datepicker.js
<p>Details</p> <p>Detected Javascript library <b>jquery-ui-dialog</b> version <b>1.10.3</b>. The version was detected from <b>file content</b>.</p> <p>References:</p> <ul style="list-style-type: none"> <li>• <a href="https://nodesecurity.io/advisories/127">https://nodesecurity.io/advisories/127</a></li> <li>• <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7103">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7103</a></li> <li>• <a href="https://www.cvedetails.com/cve/CVE-2016-7103/">https://www.cvedetails.com/cve/CVE-2016-7103/</a></li> </ul>
<p>Request headers</p> <pre>GET /crt/js/jquery.ui.datepicker.js HTTP/1.1 Accept: */* Accept-Encoding: gzip,deflate Host: nextstep.mphasis.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 Authorization: Basic bXB0YXNpc1xzcmloYXJpLnI6NmhhZnlnhJGhyZWU=</pre>

Severity	Low
Reported by module	/Scripts/PerServer/ASP_NET_Error_Message.script

## Description

The HTTP responses returned by this web application include anheader named **X-AspNet-Version**. The value of this header is used by Visual Studio to determine which version of ASP.NET is in use. It is not necessary for production sites and should be disabled.

## Impact

The HTTP header may disclose sensitive information. This information can be used to launch further attacks.

## Recommendation

Apply the following changes to the web.config file to prevent ASP.NET version disclosure:

```
<System.Web>

  <httpRuntime enableVersionHeader="false" />

</System.Web>
```

## References

[HttpRuntimeSection.EnableVersionHeader Property \(http://msdn.microsoft.com/en-us/library/system.web.configuration.httpruntime.enableversionheader.aspx\)](http://msdn.microsoft.com/en-us/library/system.web.configuration.httpruntime.enableversionheader.aspx)

## Affected items

Web Server
Details
Version information found:
4.0.30319
Request headers
GET / ~.aspx HTTP/1.1 Accept: */* Accept-Encoding: gzip,deflate Host: nextstep.mphasis.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 Authorization: Basic bXBoYXNpc1xzcmloYXJpLnI6NmhhZnlnhJGhyZWU=

## Scanned items (coverage report)

---

<https://nextstep.mphasis.com/>  
<https://nextstep.mphasis.com/crt>  
<https://nextstep.mphasis.com/crt/addTest.html>  
<https://nextstep.mphasis.com/crt/annual-t-a-plan.html>  
<https://nextstep.mphasis.com/crt/assess-impact.html>  
<https://nextstep.mphasis.com/crt/create-training-awareness-msg.html>  
<https://nextstep.mphasis.com/crt/createSurvey.html>  
<https://nextstep.mphasis.com/crt/Dashboard.html>  
<https://nextstep.mphasis.com/crt/global-compliance-practice-leader.html>  
<https://nextstep.mphasis.com/crt/issue-management.html>  
<https://nextstep.mphasis.com/crt/js>  
<https://nextstep.mphasis.com/crt/js/base.js>  
<https://nextstep.mphasis.com/crt/js/datepickr.js>  
<https://nextstep.mphasis.com/crt/js/jquery-1.3.2.js>  
<https://nextstep.mphasis.com/crt/js/jquery-1.4.2.js>  
<https://nextstep.mphasis.com/crt/js/jquery-1.9.0.min.js>  
<https://nextstep.mphasis.com/crt/js/jquery-ui-1.7.2.custom.min.js>  
<https://nextstep.mphasis.com/crt/js/jquery.sortElements.js>  
<https://nextstep.mphasis.com/crt/js/jquery.ui.datepicker.js>  
[https://nextstep.mphasis.com/crt/js/modal\\_old.js](https://nextstep.mphasis.com/crt/js/modal_old.js)  
[https://nextstep.mphasis.com/crt/js/script\\_old.js](https://nextstep.mphasis.com/crt/js/script_old.js)  
<https://nextstep.mphasis.com/crt/js/tabcontent.js>  
<https://nextstep.mphasis.com/crt/lobtester.html>  
<https://nextstep.mphasis.com/crt/LogIssue.html>  
[https://nextstep.mphasis.com/crt/MonitoringTesting\\_AnnualPlan.html](https://nextstep.mphasis.com/crt/MonitoringTesting_AnnualPlan.html)  
<https://nextstep.mphasis.com/crt/MonitoringTestingLOBTester.html>  
<https://nextstep.mphasis.com/crt/MonitoringTestingLOBTesterTestResults.html>  
<https://nextstep.mphasis.com/crt/policy-owner.html>  
[https://nextstep.mphasis.com/crt/regulatory-mgmt-compliance\\_officer.html](https://nextstep.mphasis.com/crt/regulatory-mgmt-compliance_officer.html)  
<https://nextstep.mphasis.com/crt/regulatory-mgmt.html>  
<https://nextstep.mphasis.com/crt/resources>  
<https://nextstep.mphasis.com/crt/resources/css>  
<https://nextstep.mphasis.com/crt/resources/css/images>  
<https://nextstep.mphasis.com/crt/resources/css/jquery-ui.css>  
<https://nextstep.mphasis.com/crt/resources/css/navigation.css>  
[https://nextstep.mphasis.com/crt/resources/css/style\\_annual.css](https://nextstep.mphasis.com/crt/resources/css/style_annual.css)  
<https://nextstep.mphasis.com/crt/resources/css/styles.css>  
<https://nextstep.mphasis.com/crt/resources/css/tabcontent.css>  
<https://nextstep.mphasis.com/crt/resources/css/ui.jqgrid.css>  
<https://nextstep.mphasis.com/crt/resources/fonts>  
<https://nextstep.mphasis.com/crt/resources/images>  
<https://nextstep.mphasis.com/crt/scope.html>  
<https://nextstep.mphasis.com/crt/search.html>  
<https://nextstep.mphasis.com/crt/test-manager.html>  
<https://nextstep.mphasis.com/crt/TestPlan.html>  
<https://nextstep.mphasis.com/crt/TestPlanVersion2.html>  
<https://nextstep.mphasis.com/crt/Training-coordinator-coursedetails.html>  
<https://nextstep.mphasis.com/crt/training-coordinator.html>  
<https://nextstep.mphasis.com/crt/training-coordinator2.html>  
<https://nextstep.mphasis.com/crt/training-SPOC.html>