acunetix

Developer Report

Acunetix Security Audit

20 June 2018

Generated by Acunetix

Scan of https://nextstep.mphasis.com/rem/Dashboard.html

Scan details

Scan information	
Start time	20/06/2018, 11:45:39
Start url	https://nextstep.mphasis.com/rem/Dashboard.html
Host	https://nextstep.mphasis.com/rem/Dashboard.html
Scan time	45 minutes, 5 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	4
High	0
Medium	2
Low	1
Informational	1

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
/rem/resources/scripts/jquery-1.7.1.min.js	1
/rem/resources/scripts/jquery-ui-1.8.10.custom.min.js	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

Web Server	1

Email address found

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: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
/rem/fieldwork_details.html	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

/rem/resources/scripts/jquery-1.7.1.min.js

Details

Detected Javascript library **jquery** version **1.7.1**.
The version was detected from **filename, file content**.

References:

- https://github.com/jquery/jquery/issues/2432
- http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/

Request headers

```
GET /rem/resources/scripts/jquery-1.7.1.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
Connection: Keep-alive
Authorization: Basic bXBoYXNpc1xzcmloYXJpLnI6NmhhdnlhJGhyZWU=
```

/rem/resources/scripts/jquery-ui-1.8.10.custom.min.js

Details

Detected Javascript library **jquery-ui-dialog** version **1.8.10.custom**.
The version was detected from **filename, file content**.

References:

- https://nodesecurity.io/advisories/127
- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7103
- https://www.cvedetails.com/cve/CVE-2016-7103/

Request headers

```
GET /rem/resources/scripts/jquery-ui-1.8.10.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
Connection: Keep-alive
```

```
Authorization: Basic bXBoYXNpc1xzcmloYXJpLnI6NmhhdnlhJGhyZWU=
```

ASP.NET version disclosure

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.httpruntimesection.enableversionheader.aspx)

Affected items

Web Server
Details
Version information found: `4.0.30319`
Request headers

```
GET /|~.aspx HTTP/1.1
Connection: keep-alive
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
Authorization: Basic bXBoYXNpc1xzcmloYXJpLnI6NmhhdnlhJGhyZWU=
```

Email address found

Severity	**Informational**
Reported by module	/Scripts/PerFile/Text_Search_File.script

Description

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

Impact

Email addresses posted on Web sites may attract spam.

Recommendation

Check references for details on how to solve this problem.

References

Anti-spam techniques (https://en.wikipedia.org/wiki/Anti-spam_techniques)

Affected items

/rem/fieldwork_details.html

Details

Pattern found:

```
Pasquale.Whitis@frb.ny.com
```

Request headers

```
GET /rem/fieldwork_details.html 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
Connection: Keep-alive
Authorization: Basic bXBoYXNpc1xzcmloYXJpLnI6NmhhdnlhJGhyZWU=
```

Scanned items (coverage report)

https://nextstep.mphasis.com/
https://nextstep.mphasis.com/rem
https://nextstep.mphasis.com/rem/advanced_search.html
https://nextstep.mphasis.com/rem/all_inventories_grid.html
https://nextstep.mphasis.com/rem/all_record_grid.html
https://nextstep.mphasis.com/rem/all_request_grid.html
https://nextstep.mphasis.com/rem/calendar_view.html
https://nextstep.mphasis.com/rem/create_new_request.html
https://nextstep.mphasis.com/rem/Dashboard.html
https://nextstep.mphasis.com/rem/dashboard_for_regulator.html
https://nextstep.mphasis.com/rem/data
https://nextstep.mphasis.com/rem/data/document.js
https://nextstep.mphasis.com/rem/data/styles.css
https://nextstep.mphasis.com/rem/edit_request.html
https://nextstep.mphasis.com/rem/fieldwork_details.html
https://nextstep.mphasis.com/rem/files
https://nextstep.mphasis.com/rem/files/advanced_search
https://nextstep.mphasis.com/rem/files/advanced_search/data.js
https://nextstep.mphasis.com/rem/files/advanced_search/styles.css
https://nextstep.mphasis.com/rem/files/all_inventories_grid
https://nextstep.mphasis.com/rem/files/all_inventories_grid/data.js
https://nextstep.mphasis.com/rem/files/all_inventories_grid/styles.css
https://nextstep.mphasis.com/rem/files/all_record_grid
https://nextstep.mphasis.com/rem/files/all_record_grid/data.js
https://nextstep.mphasis.com/rem/files/all_record_grid/styles.css
https://nextstep.mphasis.com/rem/files/all_request_grid
https://nextstep.mphasis.com/rem/files/all_request_grid/data.js
https://nextstep.mphasis.com/rem/files/all_request_grid/styles.css
https://nextstep.mphasis.com/rem/files/calendar_view
https://nextstep.mphasis.com/rem/files/calendar_view/data.js
https://nextstep.mphasis.com/rem/files/calendar_view/styles.css
https://nextstep.mphasis.com/rem/files/create_new_request
https://nextstep.mphasis.com/rem/files/create_new_request/data.js
https://nextstep.mphasis.com/rem/files/create_new_request/styles.css
https://nextstep.mphasis.com/rem/files/dashboard
https://nextstep.mphasis.com/rem/files/dashboard/data.js
https://nextstep.mphasis.com/rem/files/dashboard/styles.css
https://nextstep.mphasis.com/rem/files/dashboard_for_regulator
https://nextstep.mphasis.com/rem/files/dashboard_for_regulator/data.js
https://nextstep.mphasis.com/rem/files/dashboard_for_regulator/styles.css
https://nextstep.mphasis.com/rem/files/edit_request
https://nextstep.mphasis.com/rem/files/edit_request/data.js
https://nextstep.mphasis.com/rem/files/edit_request/styles.css
https://nextstep.mphasis.com/rem/files/fieldwork_details
https://nextstep.mphasis.com/rem/files/fieldwork_details/data.js
https://nextstep.mphasis.com/rem/files/fieldwork_details/styles.css
https://nextstep.mphasis.com/rem/files/inventory
https://nextstep.mphasis.com/rem/files/inventory/data.js
https://nextstep.mphasis.com/rem/files/inventory/styles.css
https://nextstep.mphasis.com/rem/files/key_personnel
https://nextstep.mphasis.com/rem/files/key_personnel/data.js
https://nextstep.mphasis.com/rem/files/key_personnel/styles.css
https://nextstep.mphasis.com/rem/files/modify_search
https://nextstep.mphasis.com/rem/files/modify_search/data.js
https://nextstep.mphasis.com/rem/files/modify_search/styles.css
https://nextstep.mphasis.com/rem/files/planned_request_grid
https://nextstep.mphasis.com/rem/files/planned_request_grid/data.js
https://nextstep.mphasis.com/rem/files/planned_request_grid/styles.css
https://nextstep.mphasis.com/rem/files/planned_requests
https://nextstep.mphasis.com/rem/files/planned_requests/data.js
https://nextstep.mphasis.com/rem/files/planned_requests/styles.css
https://nextstep.mphasis.com/rem/files/record_linkage
https://nextstep.mphasis.com/rem/files/record_linkage/data.js
https://nextstep.mphasis.com/rem/files/record_linkage/styles.css
https://nextstep.mphasis.com/rem/files/response_details
https://nextstep.mphasis.com/rem/files/response_details/data.js
https://nextstep.mphasis.com/rem/files/response_details/styles.css

https://nextstep.mphasis.com/rem/files/tasks
https://nextstep.mphasis.com/rem/files/tasks/data.js
https://nextstep.mphasis.com/rem/files/tasks/styles.css
https://nextstep.mphasis.com/rem/files/tasks_-_grid_1
https://nextstep.mphasis.com/rem/files/tasks_-_grid_1/data.js
https://nextstep.mphasis.com/rem/files/tasks_-_grid_1/styles.css
https://nextstep.mphasis.com/rem/files/tasks_-_grid_2
https://nextstep.mphasis.com/rem/files/tasks_-_grid_2/data.js
https://nextstep.mphasis.com/rem/files/tasks_-_grid_2/styles.css
https://nextstep.mphasis.com/rem/images
https://nextstep.mphasis.com/rem/images/advanced_search
https://nextstep.mphasis.com/rem/images/all_inventories_grid
https://nextstep.mphasis.com/rem/images/all_record_grid
https://nextstep.mphasis.com/rem/images/all_request_grid
https://nextstep.mphasis.com/rem/images/calendar_view
https://nextstep.mphasis.com/rem/images/create_new_request
https://nextstep.mphasis.com/rem/images/dashboard
https://nextstep.mphasis.com/rem/images/dashboard_for_regulator
https://nextstep.mphasis.com/rem/images/edit_request
https://nextstep.mphasis.com/rem/images/fieldwork_details
https://nextstep.mphasis.com/rem/images/inventory
https://nextstep.mphasis.com/rem/images/key_personnel
https://nextstep.mphasis.com/rem/images/modify_search
https://nextstep.mphasis.com/rem/images/planned_requests
https://nextstep.mphasis.com/rem/images/record_linkage
https://nextstep.mphasis.com/rem/images/response_details
https://nextstep.mphasis.com/rem/images/tasks
https://nextstep.mphasis.com/rem/images/tasks_-_grid_1
https://nextstep.mphasis.com/rem/images/tasks_-_grid_2
https://nextstep.mphasis.com/rem/inventory.html
https://nextstep.mphasis.com/rem/key_personnel.html
https://nextstep.mphasis.com/rem/modify_search.html
https://nextstep.mphasis.com/rem/planned_request_grid.html
https://nextstep.mphasis.com/rem/planned_requests.html
https://nextstep.mphasis.com/rem/plugins
https://nextstep.mphasis.com/rem/plugins/page_notes
https://nextstep.mphasis.com/rem/plugins/page_notes/page_notes.js
https://nextstep.mphasis.com/rem/plugins/page_notes/styles
https://nextstep.mphasis.com/rem/plugins/page_notes/styles/page_notes.css
https://nextstep.mphasis.com/rem/plugins/sitemap
https://nextstep.mphasis.com/rem/plugins/sitemap/sitemap.js
https://nextstep.mphasis.com/rem/plugins/sitemap/styles
https://nextstep.mphasis.com/rem/plugins/sitemap/styles/images
https://nextstep.mphasis.com/rem/plugins/sitemap/styles/sitemap.css
https://nextstep.mphasis.com/rem/record_linkage.html
https://nextstep.mphasis.com/rem/resources
https://nextstep.mphasis.com/rem/resources/css
https://nextstep.mphasis.com/rem/resources/css/axure_rp_page.css
https://nextstep.mphasis.com/rem/resources/css/default.css
https://nextstep.mphasis.com/rem/resources/css/images
https://nextstep.mphasis.com/rem/resources/css/reset.css
https://nextstep.mphasis.com/rem/resources/expand.html
https://nextstep.mphasis.com/rem/resources/images
https://nextstep.mphasis.com/rem/resources/reload.html
https://nextstep.mphasis.com/rem/resources/scripts
https://nextstep.mphasis.com/rem/resources/scripts/axure
https://nextstep.mphasis.com/rem/resources/scripts/axure/action.js
https://nextstep.mphasis.com/rem/resources/scripts/axure/adaptive.js
https://nextstep.mphasis.com/rem/resources/scripts/axure/annotation.js
https://nextstep.mphasis.com/rem/resources/scripts/axure/axQuery.js
https://nextstep.mphasis.com/rem/resources/scripts/axure/axQuery.std.js
https://nextstep.mphasis.com/rem/resources/scripts/axure/doc.js
https://nextstep.mphasis.com/rem/resources/scripts/axure/drag.js
https://nextstep.mphasis.com/rem/resources/scripts/axure/events.js
https://nextstep.mphasis.com/rem/resources/scripts/axure/expr.js
https://nextstep.mphasis.com/rem/resources/scripts/axure/flyout.js
https://nextstep.mphasis.com/rem/resources/scripts/axure/geometry.js
https://nextstep.mphasis.com/rem/resources/scripts/axure/globals.js

https://nextstep.mphasis.com/rem/resources/scripts/axure/ie.js
https://nextstep.mphasis.com/rem/resources/scripts/axure/init.temp.js
https://nextstep.mphasis.com/rem/resources/scripts/axure/legacy.js
https://nextstep.mphasis.com/rem/resources/scripts/axure/model.js
https://nextstep.mphasis.com/rem/resources/scripts/axure/move.js
https://nextstep.mphasis.com/rem/resources/scripts/axure/repeater.js
https://nextstep.mphasis.com/rem/resources/scripts/axure/sto.js
https://nextstep.mphasis.com/rem/resources/scripts/axure/style.js
https://nextstep.mphasis.com/rem/resources/scripts/axure/tree.js
https://nextstep.mphasis.com/rem/resources/scripts/axure/utils.temp.js
https://nextstep.mphasis.com/rem/resources/scripts/axure/variables.js
https://nextstep.mphasis.com/rem/resources/scripts/axure/viewer.js
https://nextstep.mphasis.com/rem/resources/scripts/axure/visibility.js
https://nextstep.mphasis.com/rem/resources/scripts/axutils.js
https://nextstep.mphasis.com/rem/resources/scripts/jquery-1.7.1.min.js
https://nextstep.mphasis.com/rem/resources/scripts/jquery-ui-1.8.10.custom.min.js
https://nextstep.mphasis.com/rem/resources/scripts/messagecenter.js
https://nextstep.mphasis.com/rem/resources/scripts/player
https://nextstep.mphasis.com/rem/resources/scripts/player/axplayer.js
https://nextstep.mphasis.com/rem/resources/scripts/player/splitter.js
https://nextstep.mphasis.com/rem/response_details.html
https://nextstep.mphasis.com/rem/tasks.html
https://nextstep.mphasis.com/rem/tasks_-_grid_1.html
https://nextstep.mphasis.com/rem/tasks_-_grid_2.html