



# CVE-2015-7609

Published on: 05/30/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:11 PM UTC

## CVE-2015-7609

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Zimbra Collaboration Suite](#) from [Synacor](#) contain the following vulnerability:

Synacor Zimbra Mail Client 8.6 before 8.6.0 Patch 5 has XSS via the error/warning dialog and email body content in Zimbra.

CVE-2015-7609 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

| Attack Vector  | Attack Complexity      | Privileges Required | User Interaction    |
|----------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b> | <b>LOW</b>             | <b>NONE</b>         | <b>REQUIRED</b>     |
| Scope          | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>CHANGED</b> | <b>LOW</b>             | <b>LOW</b>          | <b>NONE</b>         |

CVSS2 Score: **4.3 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>MEDIUM</b>     | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>NONE</b>            | <b>PARTIAL</b>    | <b>NONE</b>         |

## CVE References

| Description                                                                                            | Tags                                                                                                    | Link                                                                            |
|--------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| Fortinet Discovers Zimbra Collaboration Warning Dialog Cross-Site Scripting Vulnerability   FortiGuard | <a href="#">Third Party Advisory</a><br><a href="#">www.fortiguard.com</a><br><a href="#">text/html</a> | <a href="#">MISC</a><br><a href="#">www.fortiguard.com/zeroday/FG-VD-15-081</a> |
| Fortinet Discovers Zimbra Collaboration Email Body Cross-Site Scripting                                | <a href="#">Third Party Advisory</a>                                                                    | <a href="#">MISC</a>                                                            |

MISC  
bugzilla.zimbra.com/show\_bug.cgi?  
id=101436

**Z** MISC  
[wiki.zimbra.com/wiki/Security\\_Center](http://wiki.zimbra.com/wiki/Security_Center)

MISC  
bugzilla.zimbra.com/show\_bug.cgi?  
id=101435

There are currently no QIDs associated with this CVE

| Type        | Vendor                  | Product                                    | Version | Update | Edition | Language |
|-------------|-------------------------|--------------------------------------------|---------|--------|---------|----------|
| Application | <a href="#">Synacor</a> | <a href="#">Zimbra Collaboration Suite</a> | 8.6.0   | -      | All     | All      |
| Application | <a href="#">Synacor</a> | <a href="#">Zimbra Collaboration Suite</a> | 8.6.0   | p1     | All     | All      |
| Application | <a href="#">Synacor</a> | <a href="#">Zimbra Collaboration Suite</a> | 8.6.0   | p2     | All     | All      |
| Application | <a href="#">Synacor</a> | <a href="#">Zimbra Collaboration Suite</a> | 8.6.0   | p3     | All     | All      |
| Application | <a href="#">Synacor</a> | <a href="#">Zimbra Collaboration Suite</a> | 8.6.0   | p4     | All     | All      |
| Application | <a href="#">Synacor</a> | <a href="#">Zimbra Collaboration Suite</a> | 8.6.0   | -      | All     | All      |
| Application | <a href="#">Synacor</a> | <a href="#">Zimbra Collaboration Suite</a> | 8.6.0   | p1     | All     | All      |
| Application | <a href="#">Synacor</a> | <a href="#">Zimbra Collaboration Suite</a> | 8.6.0   | p2     | All     | All      |
| Application | <a href="#">Synacor</a> | <a href="#">Zimbra Collaboration Suite</a> | 8.6.0   | p3     | All     | All      |
| Application | <a href="#">Synacor</a> | <a href="#">Zimbra Collaboration Suite</a> | 8.6.0   | p4     | All     | All      |

cpe:2.3:a:synacor:zimbra\_collaboration\_suite:8.6.0:p1:\*:\*:\*:\*:

|                                                                |
|----------------------------------------------------------------|
| cpe:2.3:a:synacor:zimbra_collaboration_suite:8.6.0:p2:*:*:*:*: |
| cpe:2.3:a:synacor:zimbra_collaboration_suite:8.6.0:p3:*:*:*:*: |
| cpe:2.3:a:synacor:zimbra_collaboration_suite:8.6.0:p4:*:*:*:*: |

|                                                                |
|----------------------------------------------------------------|
| cpe:2.3:a:synacor:zimbra_collaboration_suite:8.6.0:p2:*:*:*:*: |
| cpe:2.3:a:synacor:zimbra_collaboration_suite:8.6.0:p3:*:*:*:*: |
| cpe:2.3:a:synacor:zimbra_collaboration_suite:8.6.0:p4:*:*:*:*: |

|                                                                |
|----------------------------------------------------------------|
| cpe:2.3:a:synacor:zimbra_collaboration_suite:8.6.0:p2:*:*:*:*: |
| cpe:2.3:a:synacor:zimbra_collaboration_suite:8.6.0:p3:*:*:*:*: |
| cpe:2.3:a:synacor:zimbra_collaboration_suite:8.6.0:p4:*:*:*:*: |

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)