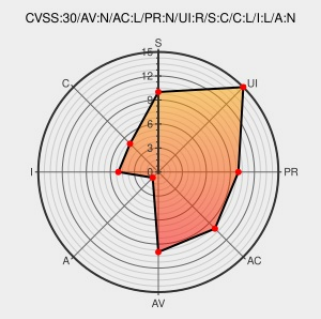
CVE-2015-7609

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 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
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Fortinet Discovers Zimbra Collaboration Warning Dialog Cross-Site Scripting Vulnerability | FortiGuard	Third Party Advisory, www.fortiguard.com, text/html	MISC www.fortiguard.com/zeroday/FG-VD-15-081
Fortinet Discovers Zimbra Collaboration Email Body Cross-Site Scripting	Third Party Advisory	MISC

Vulnerability | FortiGuard	www.fortiguard.com text/html	www.fortiguard.com/zeroday/FG-VD-15-080
Bug 101436 – Potential XSS via error/warning dialog [CWE-79]	Issue Tracking Third Party Advisory bugzilla.zimbra.com text/html	MISC bugzilla.zimbra.com/show_bug.cgi?id=101436
Security Center - Zimbra :: Tech Center	Vendor Advisory wiki.zimbra.com text/html	MISC wiki.zimbra.com/wiki/Security_Center
Bug 101435 – Persistent XSS: plain text content being rendered as a link [CWE-79]	Exploit Issue Tracking Third Party Advisory bugzilla.zimbra.com text/html	MISC bugzilla.zimbra.com/show_bug.cgi?id=101435

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Synacor	Zimbra Collaboration Suite	8.6.0	-	All	All
Application	Synacor	Zimbra Collaboration Suite	8.6.0	p1	All	All
Application	Synacor	Zimbra Collaboration Suite	8.6.0	p2	All	All
Application	Synacor	Zimbra Collaboration Suite	8.6.0	p3	All	All
Application	Synacor	Zimbra Collaboration Suite	8.6.0	p4	All	All
Application	Synacor	Zimbra Collaboration Suite	8.6.0	-	All	All
Application	Synacor	Zimbra Collaboration Suite	8.6.0	p1	All	All
Application	Synacor	Zimbra Collaboration Suite	8.6.0	p2	All	All
Application	Synacor	Zimbra Collaboration Suite	8.6.0	p3	All	All
Application	Synacor	Zimbra Collaboration Suite	8.6.0	p4	All	All

cpe:2.3:a:synacor:zimbra_collaboration_suite:8.6.0:-:*:*:*:*:*:*:

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:-:*:*:*:*:*:*:

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:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→