Zimbra Security Advisories

Zimbra Security Advisories

How to stay informed about security announcements?

You could manually check this page: https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories

And/or subscribe to the these RSS feeds (you can use Zimbra Classic UI or some other feedreader like r2e on Linux):

- https://wiki.zimbra.com/security-advisory-feed.php (no details, can be used for security notification purposes)
- https://blog.zimbra.com/feed/ (includes patches and security news with details and other news)

And subscribe to the Zeta Alliance mailing lists: https://lists.zetalliance.org/mailman/listinfo/users_lists.zetalliance.org

Overview

The following Security Vulnerabilities have been fixed and released in recent versions of Zimbra Collaboration software. For the latest release and patches, update Zimbra using your yum update or apt update. Download the latest version of our software:

- https://www.zimbra.com/product/download/

Zimbra Collaboration - Security Vulnerability Advisories

Note: only supported versions are referenced, however older unsupported versions often have the same vulnerabilities and should be upgraded to supported versions as soon as possible.
(going back to ZCS 7.1.3)

Bug#	Summary	CVE-ID	CVSS Score	Zimbra Rating	Fix Release or Patch Version	Reporter
	Restored mail rendering stability while maintaining the existing security protections.	n/a	n/a	-	10.1.16	
	Addressed an XSS vulnerability in zimbra webmail	CVE-2026-33368	TBD	-	10.1.16	Vũ
	Fixed an authenticated LDAP injection vulnerability by sanitizing user-controlled input.	CVE-2026-33369	TBD	-	10.1.16	truff, OVHCloud Bug Bounty program
	PDF attachment preview functionality has been restored in the Classic UI while maintaining security protections.	n/a	n/a	-	10.1.16	
	Addressed a stored XSS vulnerability in the Briefcase feature caused by inline rendering of specific uploaded file types when shared publicly.	CVE-2026-33370	TBD	-	10.1.16	truff, OVHCloud Bug Bounty program
	Addressed an authenticated XXE vulnerability in the EWS SOAP endpoint.	CVE-2026-33371	TBD	-	10.1.16	Research Industrial Systems Engineering (RISE)
	Fixed a CSRF validation issue where tokens were incorrectly accepted from the request body instead of the required header.	CVE-2026-33372	TBD	-	10.1.16	Ashish Kataria
	Patched a stored XSS vulnerability in the Classic UI where attackers could abuse CSS @import directives in email HTML.	CVE-2025-66376	TBD	-	10.1.13 10.0.18	NCSC-FI
	Revoked and removed hardcoded Flickr API credentials from the Flickr Zimlet.	CVE-2025-67809	TBD	-	10.1.13	Jaswanth Chemarthipalli
	Introduced path validation in the ExportAndDeleteItemsRequest API to prevent unsafe file exports.	n/a	n/a	-	10.1.13 10.0.18	devme4f from VNPT-VCI
	Addressed a missing CSRF enforcement issue in specific authentication flows.	CVE-2026-33373	TBD	-	10.1.13 10.0.18	Ashish Kataria
	Addressed an unauthenticated local file inclusion vulnerability in the RestFilter.	CVE-2025-68645	TBD	-	10.1.13 10.0.18	devme4f from VNPT-VCI
	Fixed a stored XSS vulnerability in Zimbra Mail Client for emails with PDF attachments.	n/a	n/a	-	10.1.13	Anubhav Verma
	Added input validation and null checks in the PreAuthServlet to prevent internal error disclosure on malformed requests.	n/a	n/a	-	10.1.13	
	Addressed an admin account enumeration issue.	n/a	n/a	-	10.1.13	
	Upgraded Apache HttpClient library to version 4.5.14 as a proactive security and maintenance measure.	n/a	n/a	-	10.1.13	
	Addressed a Server-Side Request Forgery (SSRF) vulnerability in the chat proxy	CVE-2025-62763	TBD	-	10.1.12	Research Industrial Systems Engineering (RISE)

configuration.					
Addressed a Cross-Site Request Forgery (CSRF) vulnerability in the ResetPasswordRequest SOAP operation by enforcing CSRF token validation.	CVE-2025-54390	TBD	-	10.0.16 10.1.10	
A security fix has been applied to require a valid auth token before allowing 2FA modifications, preventing unauthorized changes.	CVE-2025-54391	TBD	-	10.0.16 10.1.10	Ashish Kataria
Access to the GraphiQL IDE at /modern/graphiql has been disabled.			-	10.1.10	
The @babel/runtime package has been upgraded to version 7.27.6 to address a ReDoS vulnerability.	CVE-2025-27789		-	10.1.10	
The Rsync package has been upgraded to version 3.4.1 to fix multiple vulnerabilities.			-	10.1.10	
Write access to /opt/zimbra/jetty/webapps has been restricted to enhance security and mitigate potential risks.			-	10.0.16	
Addressed a denial of service (DoS) vulnerability in the admin console that could lead to service disruptions.	CVE-2025-53645		-	9.0.0 Patch 46 10.0.15 10.1.9	
This patch fixes a critical security vulnerability related to stored cross-site scripting in the Zimbra Classic Web Client. The fix strengthens input sanitization and enhances security. All customers are strongly advised to upgrade to this latest patch version immediately.	TBD	TBD	-	9.0.0 Patch 46 10.0.15 10.1.9	
Addressed a denial of service (DoS) vulnerability that could lead to service disruptions. A new local config attribute, ajax_uri_max_assets_requests_allowed has been added.	TBD		-	9.0.0 Patch 45 10.0.14 10.1.8	Nassim Abbaoui, OVHcloud
The ClamAV package has been upgraded to version 1.0.8 to fix multiple vulnerabilities.	CVE-2025-20128 5.3 CVE-2024-20505 7.5		-	10.1.8	
Write access to /opt/zimbra/jetty/webapps has been restricted to enhance security and mitigate potential risks.			-	10.1.6	
This patch fixes a critical security vulnerability related to stored cross-site scripting in the Zimbra Classic Web Client. The fix strengthens input sanitization and enhances security. All customers are strongly advised to upgrade to this latest patch version immediately.	CVE-2025-27915	TBD	-	9.0.0 Patch 44 10.0.13 10.1.5	
An SQL injection vulnerability in the ZimbraSyncService SOAP endpoint has been resolved.	CVE-2025-25064	TBD	-	10.0.12 10.1.4	byc_404 (Joe Zhou)
SSRF vulnerability in the RSS feed parser that allowed unauthorized redirection to internal network endpoints has been resolved.	CVE-2025-25065	TBD	-	9.0.0 Patch 43 10.0.12 10.1.4	Mauro Dini
A vulnerability in the ChangePassword API has been fixed to require a valid auth token.	TBD	TBD	-	9.0.0 Patch 43 10.0.12 10.1.4	Ashish Kataria
CSRF vulnerability on GraphQL endpoints allowing unauthorized operations has been	CVE-2025-32354	TBD	-	10.1.4	0xf4h1m

addressed by enforcing CSRF token validation.				9.0.0 Patch 43	
An issue with encoded @import statements in <style> tags that allowed the loading of malicious CSS has been addressed.	TBD	TBD	-	10.0.12 10.1.4 8.8.15 Patch 47	lebr0nli (Alan Li)
A Cross-Site Scripting (XSS) vulnerability via crafted <img> HTML content in the Zimbra Classic UI has been fixed. LC attribute zimbra_owasp_strip_alt_tags_with_handlers introduced in previous patch is no longer required and has been removed.	CVE-2024-45516	TBD	-	9.0.0 Patch 43 10.0.12 10.1.4 8.8.15 Patch 47	lebr0nli (Alan Li)
A Cross-Site Scripting (XSS) vulnerability via crafted HTML content in the Zimbra Classic UI has been fixed. LC attribute zimbra_owasp_strip_alt_tags_with_handlers introduced in previous patch is no longer required and has been removed.	CVE-2025-48700	TBD	-	9.0.0 Patch 43 10.0.12 10.1.4 8.8.15 Patch 47	lebr0nli (Alan Li)
A Local File Inclusion (LFI) vulnerability in the /h/rest endpoint, allowing authorized remote attackers to access sensitive files in the WebRoot using their valid auth tokens, has been fixed to prevent unauthorized file access.	CVE-2024-54663	TBD	-	10.0.11 10.1.3	lebr0nli (Alan Li)
An XSS vulnerability in the /h/rest endpoint, which allows authorized remote attackers to exploit it using their valid auth tokens, has been fixed to prevent arbitrary JavaScript execution.	CVE-2025-27914	TBD	-	10.0.11 10.1.3	lebr0nli (Alan Li)
The OpenJDK package has been upgraded to version 17.0.12 to fix multiple vulnerabilities	CVE-2023-22067	TBD	-	10.0.11 10.1.3	
The Apache package has been upgraded to version 2.4.62 to fix multiple vulnerabilities	CVE-2023-38709	TBD	-	10.0.11 10.1.3	
The ClamAV package has been upgraded to version 1.0.6 to fix multiple vulnerabilities	CVE-2024-20328	TBD	-	10.0.11 10.1.3	
Addressed a Cross-Site Request Forgery (CSRF) vulnerability by disabling GraphQL GET methods via localconfig. A new local config attribute, zimbra_gql_enable_dangerous_deprecated_get_method_will_be_removed, has been introduced to control these methods. The default value is FALSE (getting displayed as null), and customers are recommended not to set it to TRUE.	CVE-2024-9665	6.5	-	9.0.0 Patch 42 10.0.10 10.1.2	Zero Day Initiative (ZDI)
Fixed a security vulnerability in the postjournal service which may allow unauthenticated users to execute commands.	CVE-2024-45519	9.8	-	9.0.0 Patch 41 10.0.9 10.1.1 8.8.15 Patch 46	lebr0nli (Alan Li)
A Server-Side Request Forgery (SSRF) vulnerability that allowed unauthorized access to internal services has been addressed.	CVE-2024-45518	8.8	-	9.0.0 Patch 41 10.0.9 10.1.1 8.8.15 Patch 46	lebr0nli (Alan Li)
Fixed a reflected XSS vulnerability in the Briefcase module due to improper sanitization by the OnlyOffice formatter.	CVE-2024-45511	TBD	-	10.0.9 10.1.1	Noam Hamnich

Resolved Cross-Site Scripting (XSS) vulnerability due to inadequate validation of metadata's Content-Type when importing files into the briefcase, preventing arbitrary JavaScript execution.	CVE-2024-45515	TBD	-	10.0.9 10.1.1	lebr0nli (Alan Li)
A reflected XSS vulnerability in the calendar endpoint has been addressed.	CVE-2024-50599	TBD	-	8.8.15 Patch 46 9.0.0 Patch 41	Clément Lecigne of Google's Threat Analysis Group
A Cross-Site Scripting (XSS) vulnerability in TinyMCE was addressed in the upgrade from version 7.1.1 to 7.2.0	CVE-2024-38356	TBD	-	10.0.9 10.1.1	
Fixed a stored XSS vulnerability that could lead to unauthorized actions when adding contacts from specially crafted emails.	CVE-2024-45510	TBD	-	9.0.0 Patch 41 10.0.9 10.1.1	Elweth
Fixed a Stored Cross-Site Scripting (XSS) vulnerability in the Briefcase module that could execute malicious code when interacting with folder share notifications.	CVE-2024-45512	TBD	-	9.0.0 Patch 41 10.0.9 10.1.1	Noam Hamnich
A Cross-Site Scripting (XSS) vulnerability caused by a non-sanitized `packages` parameter has been resolved.	CVE-2024-45514	TBD	-	9.0.0 Patch 41 10.0.9 10.1.1 8.8.15 Patch 46 9.0.0 Patch 41	lebr0nli (Alan Li)
A Cross-Site Scripting (XSS) vulnerability in the `/h/rest` endpoint has been fixed.	CVE-2024-45517	TBD	-	10.0.9 10.1.1 8.8.15 Patch 46 9.0.0 Patch 41	lebr0nli (Alan Li)
A Cross-Site Scripting (XSS) issue that allowed an attacker to inject and execute malicious code via email account configurations has been resolved.	CVE-2024-45194	TBD	-	10.0.9 10.1.1 9.0.0 Patch 41	Noam Hamnich
A stored XSS vulnerability in the `contacts/print` endpoint has been addressed.	CVE-2024-45513	TBD	-	10.0.9 10.1.1	0xf4h1m
A security vulnerability in Zimbra Desktop 4.38.0 has been addressed where remote attackers could exploit a flaw to read arbitrary files by tricking users into opening a malicious email and clicking a link.	TBD	TBD	-	4.39.0	lebr0nli (Alan Li)
Removed the use of Node integration from the Electron framework used in Modern Zimbra Desktop that allowed remote code execution, preventing Node.js code from being executed in the renderer process.	TBD	TBD	-	4.38.0	lebr0nli (Alan Li)
Upgraded Electron framework used in Modern Zimbra Desktop to version 28.0.0, This update mitigates potential security risks associated with the outdated Electron version 11.5.0.	CVE-2023-4863	8.8	-	4.38.0	
Upgraded graphiql from version 3.1.0 to 3.2.0 to address a high severity infinite loop vulnerability.	TBD	TBD	-	10.1.0	
Addressed a high severity Prototype Pollution vulnerability in Modern UI. The concerned library has been removed from the codebase, and a custom utility function	TBD	TBD	-	10.1.0	

has been implemented to achieve the same functionality, mitigating the vulnerability.					
SMTP Smuggling vulnerability Patched	CVE-2023-51764	5.3	-	9.0.0 Patch 40 10.0.8	
Upgraded PHP to 8.3.0 to fix allocated memory vulnerability	CVE-2021-21708	9.8	-	9.0.0 Patch 40 10.0.8	
An XSS vulnerability was observed due to the execution of malicious JavaScript code from an externally shared file via non-sanitized parameter	CVE-2024-33536	5.4	-	9.0.0 Patch 40 10.0.8 8.8.15 Patch 46	Netragard
Unauthenticated Local File Inclusion in zimbraAdmin interface via "packages" parameter	CVE-2024-33535	7.5	-	9.0.0 Patch 40 10.0.8 8.8.15 Patch 46	Netragard
Addressed XSS vulnerability in zimbraAdmin interface due to non sanitised parameter	CVE-2024-33533	5.4	-	9.0.0 Patch 40 10.0.8	Netragard
Nginx has been upgraded to version 1.24.0 to fix multiple vulnerabilities	CVE-2022-41741 CVE-2022-41742	7.8	-	9.0.0 Patch 39 10.0.7	
An XSS vulnerability in a Calendar invite has been resolved	CVE-2024-27443	6.1	-	9.0.0 Patch 39 10.0.7 8.8.15 Patch 46	nhiephon, chung96vn, SPT from NCSC Vietnam
Local Privilege Escalation vulnerability Patched	CVE-2024-27442	7.8	-	9.0.0 Patch 39 10.0.7	ZDI
OpenJDK has been upgraded to version 17.0.8 to fix multiple vulnerabilities.	CVE-2023-21930 CVE-2022-21476 CVE-2022-21449	High	-	9.0.0 Patch 38 8.8.15 Patch 45 10.0.6	
Fixed a vulnerability where an auth token was possible to be obtained.	CVE-2023-48432	6.1	-	9.0.0 Patch 38 8.8.15 Patch 45 10.0.6	Nguyễn Khắc Huy
Certbot now adopts ECDSA secp256r1 (P-256) certificate private keys as the default for all newly generated certificates. Zimbra has also introduced support for ECDSA secp256r1 (P-256) certificate private keys in new certificates.	TBD	TBD	-	9.0.0 Patch 38 8.8.15 Patch 45 10.0.6	
Modern UI was vulnerable to DOM-based Javascript injection. Security related issues have been fixed to prevent it.	TBD	TBD	-	9.0.0 Patch 38 10.0.6	
A security related issue has been fixed to prevent javascript injection through help files.	CVE-2007-1280	4.3	-	9.0.0 Patch 37 8.8.15 Patch 44 10.0.5	
A security related issue has been fixed which impacted one of the third party libraries being used in Admin User Inferface.	CVE-2020-7746	High	-	9.0.0 Patch 37 8.8.15 Patch 44 10.0.5	
An XSS vulnerability was observed when a PDF containing malicious Javascript code was uploaded in Briefcase.	CVE-2023-45207	6.1	-	9.0.0 Patch 37 8.8.15 Patch 44 10.0.5	Ramin: https://twitter.com/realraminfp, https://github.com/raminfp
Multiple possible cross-site scripting (XSS) vulnerabilities were observed in the robohelp package. The package has now been made optional. This means that users	CVE-2023-45206	6.1	-	9.0.0 Patch 37 8.8.15 Patch 44	Aviva Lietuva, UAGDPB

will now be access help documentation at the URL - https://www.zimbra.com/documentation/.				10.0.5	
XSS on one of the web endpoint via non sanitised input parameter.	CVE-2023-43103	6.1	-	9.0.0 Patch 36 8.8.15 Patch 43 10.0.4	Sk4nd4 : https://twitter.com/Sk4nd4
An attacker can gain access of logged-in user's mailbox through XSS.	CVE-2023-43102	6.1	-	9.0.0 Patch 36 8.8.15 Patch 43 10.0.4	Florian Klaar
Bug that could allow an unauthenticated attacker to gain access to a Zimbra account.	CVE-2023-41106	8.8	-	9.0.0 Patch 35 8.8.15 Patch 42 10.0.3	Sk4nd4 : https://twitter.com/Sk4nd4
A cross-site scripting (XSS) vulnerability that was present in the in the Zimbra Classic Web Client has been addressed.	CVE-2023-37580	6.1	-	8.8.15 Patch 41	Clement Lecigne, Google's Threat Analysis Group
OpenSSL package has been upgraded to fix a security issue related to the verification of X.509 certificate chains that include policy constraints	CVE-2023-0464	7.5	-	9.0.0 Patch 34 8.8.15 Patch 41 10.0.2	
The Amavis package has been upgraded to 2.13.0 version.	TBD	TBD	-	9.0.0 Patch 34 8.8.15 Patch 41 10.0.2	
A bug that could lead to exposure of internal JSP and XML files has been fixed.	CVE-2023-38750	7.5	-	9.0.0 Patch 34 8.8.15 Patch 41 10.0.2	
A possible Cross-site Scripting (XSS) security vulnerability has been fixed	CVE-2023-34192	9.0	High	8.8.15 Patch 40	Skay, Noah-Lab
As part of continuous improvement, ClientUploader packages has been removed from core product and moved to an optional package	CVE-2023-34193	8.9	Medium	Daffodil 10.0.1 9.0.0 Patch 33 8.8.15 Patch 40	Rudransh Jani of Ownux Global
The Apache package has been upgraded to version 2.4.57 to fix multiple vulnerabilities	CVE-2023-25690	9.8	Low	Daffodil 10.0.1 9.0.0 Patch 33 8.8.15 Patch 40	Jabetto
Remove unused JSP file which may bypass the Preauth verification	CVE-2023-29382	9.8	Low	Daffodil 10.0.1 9.0.0 Patch 33 8.8.15 Patch 40	Skay, Noah-Lab
The Apache CXF package has been upgraded to version 3.5.5 to fix SSRF vulnerability	CVE-2022-46364	9.8	Low	Daffodil 10.0.1 9.0.0 Patch 33 8.8.15 Patch 40	Atos Worldline
The Spring Core package has been upgraded to version 6.0.8 to fix multiple vulnerabilities	CVE-2022-22971 CVE-2022-22970 CVE-2022-22971	5.3	Low	Daffodil 10.0.1 9.0.0 Patch 33 8.8.15 Patch 40	Stuart Williamson, Visa Digital Ticketing
Added additional validations for 2FA login.	CVE-2023-29381	9.8	Medium	Daffodil 10.0.1 9.0.0 Patch 33 8.8.15 Patch 40	Technik BNV-GZ
The ClamAV package has been upgraded to version 0.105.2 to fix multiple vulnerabilities.	CVE-2023-20032	9.8	High	9.0.0 Patch 31 8.8.15 Patch 38	
Multiple security issues related possibility of RXSS attack related to printing messages and appointments have been fixed.	CVE-2023-24031	6.1	Low	9.0.0 Patch 30	Marco Ortisi Valentin T.
The OpenSSL package has been upgraded to version 8.7b4 to fix multiple vulnerabilities.	CVE-2023-0286	7.4	Low	9.0.0 Patch 30 8.8.15 Patch 37	
Strengthened PreAuth servlet to only redirect to admin configured url, which will	CVE-2023-24030	6.1	Low	9.0.0 Patch 30 8.8.15 Patch 37	Ali Dinifar

	prevent security issues related to open redirection vulnerabilities.					
	Previously, the account status was not validated when sending emails using 2FA. Added additional validations for user accounts to check the account status and allow email operations.	CVE-2023-26562	7.8	Medium	9.0.0 Patch 30 8.8.15 Patch 37	
	Strengthened security of Zimbra product by disallowing usage of some JVM arguments in mailbox manager.	CVE-2023-24032	7.8	Low	9.0.0 Patch 30 8.8.15 Patch 37	Ali Dinifar
	The Perl compress zlib package has been upgraded to version 2.103-1 to fix out-of-bounds access vulnerability.	CVE-2018-25032	7.5	Low	9.0.0 Patch 30 8.8.15 Patch 37	
	XSS can occur in Classic UI login page by injecting arbitrary javascript code.	CVE-2022-45911	6.1	Low	9.0.0 Patch 28	National Examinations Council of Tanzania (NECTA)
	RCE through ClientUploader from authenticated admin user.	CVE-2022-45912	7.2	Medium	9.0.0 Patch 28 8.8.15 Patch 35	Strio
	XSS can occur via one of attribute in webmail urls, leading to information disclosure.	CVE-2022-45913	6.1	Medium	9.0.0 Patch 28 8.8.15 Patch 35	Kim Yong-Jin
	The Apache package has been upgraded to version 2.4.54 to fix multiple vulnerabilities.	CVE-2022-26377	7.5	Medium	9.0.0 Patch 28 8.8.15 Patch 35	
	The ClamAV package has been upgraded to version 0.105.1-2 to fix multiple vulnerabilities.	CVE-2022-20770 CVE-2022-20771	7.5	Low	9.0.0 Patch 28 8.8.15 Patch 35	
	YUI dependency is removed from WebClient and Admin Console.	CVE-2013-6780	TBD	Medium	9.0.0 Patch 28	
80716	An attacker can use cpio package to gain incorrect access to any other user accounts. Zimbra recommends pax over cpio.	CVE-2022-41352	9.8	Major	9.0.0 Patch 27 8.8.15 Patch 34	Yeak Nai Siew
	Zimbra's sudo configuration permits the zimbra user to execute the zmslapd binary as root with arbitrary parameters.	CVE-2022-37393	7.8	Medium	9.0.0 Patch 27 8.8.15 Patch 34	Darren Martyn
	XSS can occur via one of the attribute of an IMG element, leading to information disclosure.	CVE-2022-41348	6.1	Medium	9.0.0 Patch 27	Synacktiv
	XSS can occur via one of attribute in search component of webmail, leading to information disclosure.	CVE-2022-41350	6.1	Medium	8.8.15 Patch 34	Tin Pham aka TF1T of VietSunshine Cyber Security Services
	XSS can occur via one of attribute in compose component of webmail, leading to information disclosure.	CVE-2022-41349	6.1	Medium	8.8.15 Patch 34	Tin Pham aka TF1T of VietSunshine Cyber Security Services
	XSS can occur via one of attribute in calendar component of webmail, leading to information disclosure.	CVE-2022-41351	6.1	Medium	8.8.15 Patch 34	Tin Pham aka TF1T of VietSunshine Cyber Security Services
	Upgraded OpenSSL to 1.1.1q avoid multiple vulnerabilities.		9.8	Low	9.0.0 Patch 26 8.8.15 Patch 33	Upstream, see CVE-2022-2068
	Authentication Bypass in MailboxImportServlet.	CVE-2022-37042	9.8	High	9.0.0 Patch 26 8.8.15 Patch 33	Steven Adair and Thomas Lancaster of Volexity
109447	Proxy Servlet SSRF Vulnerability.	CVE-2022-37041	7.5	Low	9.0.0 Patch 26 8.8.15 Patch 33	Nicolas VERDIER of onepoint
	When using preauth, CSRF tokens are not checked on some post endpoints.	CVE-2022-37043	5.7	Low	9.0.0 Patch 26 8.8.15 Patch 33	Telenet security team
	Cyrus SASL package has been upgraded to version 2.1.28.		8.8	Low	9.0.0 Patch 26 8.8.15 Patch 33	Upstream, see CVE-2022-24407
	RXSS on '/h/search' via title parameter	CVE-2022-37044	6.1	Low	8.8.15 Patch 33	
	RXSS on '/h/search' via onload parameter	CVE-2022-37044	6.1	Low	8.8.15 Patch 33	
	RXSS on '/h/search' via extra parameter	CVE-2022-37044	6.1	Low	8.8.15 Patch 33	
	Upgraded Log4j to v2.		10.0	Low	9.0.0 Patch 25 8.8.15 Patch 32	Upstream, see CVE-2021-44228, CVE-2021-45105, CVE-2019-17571

	Upgraded OpenSSL to 1.1.1n to avoid DoS vulnerability.		7.5	Low	9.0.0 Patch 25 8.8.15 Patch 32	Upstream, see CVE-2022-0778
	Upgraded Jetty to 9.4.46 to avoid vulnerability due to large TLS packets causing 100% CPU usage.		7.5	Low	9.0.0 Patch 25 8.8.15 Patch 32	Upstream, see CVE-2021-28165
	Upgraded mina-core to version 2.1.6.		7.5	Low	9.0.0 Patch 25 8.8.15 Patch 32	Upstream, see CVE-2019-0231
	Memcached poisoning with unauthenticated request.	CVE-2022-27924	7.5	Medium	9.0.0 Patch 24 8.8.15 Patch 31	Simon Scannell of Sonarsource
	RCE through mboximport from authenticated user.	CVE-2022-27925	7.2	Medium	9.0.0 Patch 24 8.8.15 Patch 31	Mikhail Klyuchnikov of Positive Technologies
	XSS vulnerability in calendar in classic html client using /h/calendar.	CVE-2022-24682	6.1	Medium	8.8.15 Patch 30	Steven Adair and Thomas Lancaster of Volexity
	Proxy Servlet Open Redirect Vulnerability	CVE-2021-35209	9.8	Medium	9.0.0 Patch 16 8.8.15 Patch 23	Simon Scannell of Sonarsource
	Open Redirect Vulnerability in preauth servlet	CVE-2021-34807	6.1	Low	9.0.0 Patch 16 8.8.15 Patch 23	Simon Scannell of Sonarsource
	Stored XSS Vulnerability in ZmMailMsgView.java	CVE-2021-35208	5.4	Medium	9.0.0 Patch 16 8.8.15 Patch 23	Simon Scannell of Sonarsource
	XSS vulnerability in Zimbra Web Client via loginErrorCode	CVE-2021-35207	6.1	Medium	9.0.0 Patch 16 8.8.15 Patch 23	
	Heap-based buffer overflow vulnerabilities in PHP < 7.3.10		9.8	Critical	9.0.0 Patch 13	Upstream, see CVE-2019-9641, CVE-2019-9640
	Heap-based buffer overflow vulnerabilities in PHP < 7.3.10		9.8	Critical	8.8.15 Patch 20	Upstream, see CVE-2019-9641, CVE-2019-9640
	Upgraded Apache to 2.4.46 to avoid multiple vulnerabilities.		7.8	High	9.0.0 Patch 13	Upstream, see CVE-2019-0211, CVE-2019-0217
	Upgraded Apache to 2.4.46 to avoid multiple vulnerabilities.		7.8	High	8.8.15 Patch 20	Upstream, see CVE-2019-0211, CVE-2019-0217
	XXE (CWE-776) vulnerability in saml consumer store servlet (Network Edition)	CVE-2020-35123	6.5	Medium	9.0.0 Patch 10	Primerica
	XXE (CWE-776) vulnerability in saml consumer store servlet (Network Edition)	CVE-2020-35123	6.5	Medium	8.8.15 Patch 17	Primerica
	XSS CWE-79 vulnerability in tinymce	n/a	6.1	Medium	9.0.0 Patch 5	Upstream, see CVE-2019-1010091
	Memory Leak in nodejs library mem	n/a	5.5	Medium	9.0.0 Patch 5	Upstream, see WS-2018-0236
	Persistent XSS	CVE-2020-13653	6.1	Minor	8.8.15 Patch 11 9.0.0 Patch 4	Telenet
	Unrestricted Upload of File with Dangerous Type CWE-434	CVE-2020-12846	6.0	Minor	8.8.16 Patch 10 9.0.0 Patch 3	Telenet
	Persistent XSS CWE-79	CVE-2020-11737	4.3	Minor	9.0.0 Patch 2	Zimbra
109174	Non-Persistent XSS CWE-79	CVE-2019-12427	4.3	Minor	8.8.15 Patch 1	Meridian Miftari
109141	Non-Persistent XSS CWE-79	CVE-2019-15313	4.3	Minor	8.8.15 Patch 1	Quang Bui
109124	Non-Persistent XSS CWE-79	CVE-2019-8947	2.6	Minor	-	Issam Rabhi of Sysdream
109123	Persistent XSS CWE-79	CVE-2019-8946	2.6	Minor	-	Issam Rabhi of Sysdream
109122	Persistent XSS CWE-79	CVE-2019-8945	3.5	Minor	-	Issam Rabhi of Sysdream
109117	Persistent XSS CWE-79	CVE-2019-11318	3.5	Minor	8.8.12 Patch 1	Mondher Smii
109127	SSRF CWE-918 / CWE-807	CVE-2019-9621	4.0	Minor	8.7.11 Patch11 8.8.9 Patch10 8.8.10 Patch8 8.8.11 Patch4 8.8.12	An Trinh
109096	Blind SSRF CWE-918	CVE-2019-6981	4.0	Minor	8.7.11 Patch11 8.8.9 Patch10 8.8.10 Patch8 8.8.11 Patch4 8.8.12	An Trinh
109129	XXE CWE-611 (8.7.x only)	CVE-2019-9670	6.4	Major	8.7.11 Patch10	Khanh Van Pham An Trinh

109097	Insecure object deserialization CWE-502	CVE-2019-6980	5.4	Major	8.7.11 Patch9 8.8.9 Patch10 8.8.10 Patch7 8.8.11 Patch3 8.8.12	An Trinh
109093	XXE CWE-611	CVE-2018-20160	6.4	Major	8.7.x see 109129 above 8.8.9 Patch9 8.8.10 Patch5 8.8.11 Patch1 8.8.12	An Trinh
109017	Non-Persistent XSS CWE-79	CVE-2018-14013	4.3	Minor	8.7.11 Patch8 8.8.9 Patch9 8.8.10 Patch5 8.8.11	Issam Rabhi of Sysdream
109020	Persistent XSS CWE-79	CVE-2018-18631	5.0	Major	8.7.11 Patch7 8.8.9 Patch7 8.8.10 Patch2 8.8.11	Netragard
109018	Non-Persistent CWE-79	CVE-2018-14013	2.6	Minor	8.7.11 Patch7 8.8.9 Patch6 8.8.10 Patch1 8.8.11	Issam Rabhi of Sysdream
109021	Limited Content Spoofing CWE-345	CVE-2018-17938	4.3	Minor	8.8.10	Sumit Sahoo
109012	Account Enumeration CWE-203	CVE-2018-15131	5.0	Major	8.7.11 Patch6 8.8.8 Patch9 8.8.9 Patch3	Danielle Deibler
108970	Persistent XSS CWE-79	CVE-2018-14425	3.5	Minor	8.8.8 Patch7 8.8.9 Patch1	Diego Di Nardo
108902	Persistent XSS CWE-79	CVE-2018-10939	3.5	Minor	8.6.0 Patch11 8.7.11 Patch4 8.8.8 Patch4	Diego Di Nardo
108963	Verbose Error Messages CWE-209	CVE-2018-10950	3.5	Minor	8.7.11 Patch3 8.8.8	Netragard
108962	Account Enumeration CWE-203	CVE-2018-10949	5.0	Major	8.7.11 Patch3 8.8.8	Netragard
108894	Persistent XSS CWE-199	CVE-2018-10951	3.6	Minor	8.6.0 Patch10 8.7.11 Patch3 8.8.8	Netragard
97579	CSRF CWE-352	CVE-2015-7610	5.8	Major	8.6.0 Patch10 8.7.11 Patch2 8.8.8 Patch1	Fortinet's FortiGuard Labs
108786	Persistent XSS CWE-79	CVE-2018-6882	4.3	Minor	8.6.0 Patch10 8.7.11 Patch1 8.8.7 8.8.8	Stephan Kaag of Securify
108265	Persistent XSS CWE-79	CVE-2017-17703	4.3	Minor	8.6.0 Patch9 8.7.11 Patch1 8.8.3	Veit Hailperin
107963	Host header injection CWE-20	-	4.3	Minor	8.8.0 Beta2	-
107948 107949	Persistent XSS CWE-79	CVE-2018-10948	3.5	Minor	8.6.0 Patch10 8.7.11 Patch3 8.8.0 Beta2	Lucideus Phil Pearl
107925	Persistent XSS - snippet CWE-79	CVE-2017-8802	3.5	Minor	8.6.0 Patch9 8.7.11 Patch1 8.8.0 Beta2	Compass Security
107878	Persistent XSS - location CWE-79	CVE-2017-8783	4.0	Minor	8.7.10	Stephan Kaag of Securify
107712	Improper limitation of file paths CWE-22	CVE-2017-6821	4.0	Minor	8.7.6	Greg Solovyev, Phil Pearl
107684	Improper handling of privileges CWE-280	CVE-2017-6813	4.0	Major	8.6.0 Patch9 8.7.6	Greg Solovyev

106811	XXE CWE-611	CVE-2016-9924	5.8	Major	8.6.0 Patch10 8.7.4	Alastair Gray
106612	Persistent XSS CWE-79	CVE-2017-7288	4.3	Minor	8.6.0 Patch11 8.7.1	Sammy Forgit
105001 105174	XSS CWE-79	CVE-2016-5721	4.3 2.1	Minor	8.6.0 Patch11 8.7.0	Secu
104552 104703	XSS CWE-79	CVE-2016-3999	4.3	Minor	8.7.0	Nam Habach
104477	Open Redirect CWE-601	CVE-2016-4019	4.3	Minor	8.7.0	Zimbra
104294 104456	CSRF CWE-352	CVE-2016-3406	2.6	Minor	8.6.0 Patch8 8.7.0	Zimbra
104222 104910 105071 105175 103997	XSS CWE-79	CVE-2016-3407	4.3 3.5 4.3 2.1	Minor	8.6.0 Patch11 8.7.0	Zimbra
104413 104414 104777 104791	XSS CWE-79	CVE-2016-3412	3.5	Minor	8.7.0	Zimbra
103996	XXE (Admin) CWE-611-	CVE-2016-3413	2.6	Minor	8.6.0 Patch11 8.7.0	Zimbra
103961 104828	CSRF CWE-352	CVE-2016-3405	4.3	Minor	8.6.0 Patch8 8.7.0	Zimbra
103959	CSRF CWE-352	CVE-2016-3404	4.3	Minor	8.6.0 Patch8 8.7.0	Zimbra
103956 103995 104475 104838 104839	XSS CWE-79	CVE-2016-3410	4.3	Minor	8.6.0 Patch11 8.7.0	Zimbra
103609	XSS CWE-79	CVE-2016-3411	3.5	Minor	8.6.0 Patch11 8.7.0	Zimbra
102637	XSS CWE-79	CVE-2016-3409	4.3	Minor	8.6.0 Patch11 8.7.0	Peter Nguyen
102276	Deserialization of Untrusted Data CWE-502	CVE-2016-3415	5.8	Major	8.7.0	Zimbra
102227	Deserialization of Untrusted Data CWE-502	n/a	7.5	Major	8.7.0	Upstream, see CVE-2015-4852
102029	CWE-674	CVE-2016-3414	4.0	Minor	8.6.0 Patch7 8.7.0	Zimbra
101813	XSS CWE-79	CVE-2016-3408	4.3	Minor	8.6.0 Patch11 8.7.0	Volexity
100885 100899	CSRF CWE-352	CVE-2016-3403	5.8	Major	8.6.0 Patch8 8.7.0	Sysdream
99810	CWE-284 CWE-203	CVE-2016-3401	3.5	Minor	8.7.0	Zimbra
99167	Account Enumeration CWE-203	CVE-2016-3402	2.6	Minor	8.7.0	Zimbra
101435 101436 101559	Persistent XSS CWE-79	CVE-2015-7609	6.4 2.3	Major	8.6.0 Patch5 8.7.0	Fortinet's FortiGuard Labs
100133 99854 99914 96973	XSS CWE-79	CVE-2015-2249	3.5	Minor	8.6.0 Patch5 8.7.0	Zimbra
99236	XSS Vuln in YUI components in ZCS	n/a	4.3	Minor	8.6.0 Patch5	Upstream, see CVE-2012-5881

						CVE-2012-5882 CVE-2012-5883
98358						
98216	Non-Persistent XSS CWE-79	CVE-2015-2249	4.3	Minor	8.6.0 Patch2 8.7.0	Cure53
98215						
97625	Non-Persistent XSS CWE-79	CVE-2015-2230	3.5	Minor	8.6.0 Patch2	MWR InfoSecurity
96105	Improper Input Validation CWE-20	CVE-2014-8563	5.8	Major	8.0.9 8.5.1 8.6.0	-
83547	CSRF Vulnerability CWE-352	CVE-2015-6541	5.8	Major	8.5.0	iSEC Partners, Sysdream
87412						
92825 92833	XSS Vulnerabilities CWE-79 (8.0.7 Patch contains 87412)	CVE-2014-5500	4.3	Minor	8.0.8 8.5.0	-
92835						
83550	Session Fixation CWE-384	CVE-2013-5119	5.8	Major	8.5.0	-
91484	Patch ZCS8 OpenSSL for CVE-2014-0224	n/a	6.8	Major	8.0.3+Patch 8.0.4+Patch 8.0.5+Patch 8.0.6+Patch 8.0.7+Patch	Upstream, see CVE-2014-0224
88708	Patch ZCS8 OpenSSL for CVE-2014-0160	n/a	5.0	Major	8.0.3+Patch 8.0.4+Patch 8.0.5+Patch 8.0.6+Patch 8.0.7+Patch 8.0.7	Upstream, see CVE-2014-0160
85499	Upgrade to OpenSSL 1.0.1f	n/a	4.3 4.3 5.8	Major	8.0.7	Upstream, see CVE-2013-4353 CVE-2013-6449 CVE-2013-6450
84547	XXE CWE-611	CVE-2013-7217	6.4 (not 10.0)	Critical	7.2.2_Patch3 7.2.3_Patch 7.2.4_Patch2 7.2.5_Patch 7.2.6 8.0.3_Patch3 8.0.4_Patch2 8.0.5_Patch 8.0.6	Private
85478	XSS vulnerability in message view	-	6.4	Major	8.0.7	Alban Diquet of iSEC Partners
85411	Local root privilege escalation	-	6.2	Major	8.0.7	Matthew David
85000	Patch nginx for CVE-2013-4547	n/a	7.5	Major	7.2.7 8.0.7	Upstream, see CVE-2013-4547
80450 80131 80445 80132	Upgrade to JDK 1.6 u41 Upgrade OpenSSL to 1.0.0k Upgrade to JDK 1.7u15+ Upgrade to OpenSSL 1.0.1d	n/a	2.6	Minor	7.2.3 7.2.3 8.0.3 8.0.3	Upstream, see CVE-2013-0169
80338	Local file inclusion via skin/branding feature CWE-22	CVE-2013-7091	5.0	Critical	6.0.16_Patch 7.1.1_Patch6 7.1.3_Patch3 7.2.2_Patch2 7.2.3 8.0.2_Patch 8.0.3	Private
77655	Separate keystore for CAs used for X509 authentication	-	5.8	Major	8.0.7	Private

75424	Upgrade to Clamav 0.97.5	n/a	4.3 4.3 4.3	Minor	7.2.1	Upstream, see CVE-2012-1457 CVE-2012-1458 CVE-2012-1459
64981	Do not allow HTTP GET for login	-	6.8	Major	7.1.3_Patch 7.1.4	Private

Try Zimbra

Try now Zimbra Collaboration without any cost with the 60-day free Trial.

Want to get involved?

You can contribute in the Community, in the Wiki, in the Code, or developing Zimlets.
Find out more. »

Other Help Resources

Looking for a Video?

Visit our YouTube Channel to keep posted about Webinars, technology news, Product overviews and more.

Retrieved from "http://wiki.zimbra.com/index.php?title=Zimbra_Security_Advisories&oldid=71375"
Jump to: navigation, search

Products

Zimbra Collaboration
Zimbra 8.8.15
Zimbra Cloud
Zimbra Open Source
Compare Products
Pricing
What's New
Downloads

Support

Overview
Zimbra Support Offerings
Professional Services
User Help
Customer Support Portal

Learn

What is Zimbra?
Demos and Videos
Case Studies
About Us

Community

Forums
Documentation

Blog
Submit a ticket