



Soheil SamanAbadi

Follow

Jul 8 · 3 min read · [Listen](#)



Save



Zimbra 8.8.15 zmprove ca command Incorrect Access Control

> Hi everyone.

>

> [Suggested description]

> Zimbra Collaboration Open Source 8.8.15 does not encrypt the initial-login

> randomly created password (from the “zmprove ca” command). It is visible

> in cleartext on port UDP 514 (aka the Syslog port).

>

The screenshot displays the ManageEngine EventLog Analyzer interface. The search results show several log entries for Zimbra login attempts. Each entry includes the following details:

- Message:** root: TTY=unknown; PWD=/opt/sample; USER=zimbra; COMMAND=/opt/zimbra/bin/zmprove ca k.tale [redacted] [redacted]
- Time:** 2022-05-08 23:46:06, 2022-05-08 23:46:18, 2022-05-08 23:46:16, 2022-05-08 23:46:12, 2022-05-08 23:45:01
- Device:** uMail
- Severity:** notice
- Facility:** AuthPriv
- Source:** sudo
- Username:** root
- Remote Device:** [redacted]
- LogType:** Unix
- Display Name:** uMail

The interface also includes a navigation bar with options like Home, Reports, Compliance, Search, Correlation, Alerts, Settings, LogMe, and Support. A search bar is visible at the top, and a 'Log Search' button is on the right. The bottom of the screen shows a mobile navigation bar with icons for home, search, and profile.



[Open in app](#)

[Get started](#)

> [Vulnerability Type]
> Incorrect Access Control
>
> -----
>
> [Vendor of Product]
> Zimbra
>
> -----
>
> [Affected Product Code Base]
> Zimbra Collaboration Open Source — Zimbra 8.8.15
>
> -----
>
> [Affected Component]
> “zimbra/zmprove ca” command
>
> -----
>
> [Attack Type]
> Remote
>
> -----
>
> [Impact Escalation of Privileges]
> true
>
> -----
>
> [Impact Information Disclosure]





Open in app

Get started

> [CVE Impact Other]

> Default user/password

>

> -----

>

> [Attack Vectors]

> when an user created with “zmprove ca” command in zimbra, a random

> password will generate with it. but, when an eavesdropper listening to

> port UDP 514 aka Syslog port, the password can be seen in clear text

> with “COMMAND=zimbra/zmprove ca username and password” format.

> admin can active most change password option but it's not enough.

>

> -----

>

> [Reference]

> <https://medium.com/@soheil.samanabadi/zimbra-8-8-15-zmprove-ca-command-incorrect-access-control-8088032638e>

> <https://github.com/soheilsamanabadi/vulnerabilitys/blob/main/Zimbra%208.8.15%20zmprove%20ca%20command>

> <https://www.zimbra.com/downloads/>

> https://wiki.zimbra.com/wiki/Security_Center

> https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories

>

> -----

> > [Timelines]

> 1. Report to Zimbra on Jun, 2022

>

> [Discoverer]

> Soheil Samanabadi , Ali Ahmadi

> [linkedin.com/in/soheil-samanabadi/](https://www.linkedin.com/in/soheil-samanabadi/)





Open in app

Get started

[About](#) [Help](#) [Terms](#) [Privacy](#)

Get the Medium app

