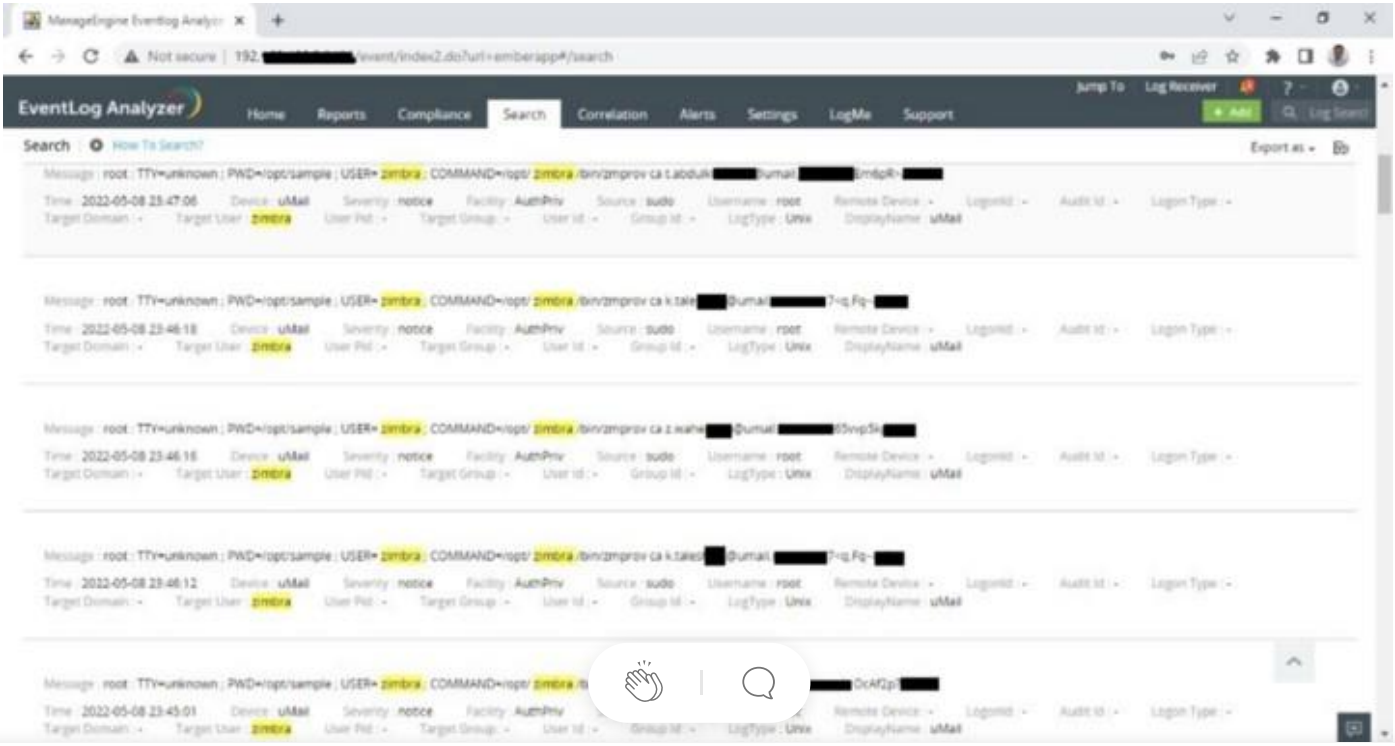
Soheil SamanAbadi Follow

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).
>



> [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]

> [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/

Open in app Get started

About Help Terms Privacy

Get the Medium app