Advisory	**ADE-2021-01**		September 16, 2021
Manufacturer	Red Hat	Product	Keycloak
Affected Version(s)	15.0.0	Tested Version(s)	15.0.0
CWE	208, 640	CVE	-
Risk	Medium	Status	Reported

Overview

Keycloak is an open source software product for single sign-on and Identity and Access Management. Keycloak is one of the most widely used tools in the enterprise sector.

One of the base functionality of Keycloak is to allow password recovery via email. That password recovery feature seems to be synchronous. This leads to an observable timing discrepancy when recovering passwords of existing and non-existing user accounts.

Vulnerability Details

When recovering a password an email is sent and the user gets the feedback that he or she should receive an email shortly with further instructions. Doesn't matter if the user exists or not.

When recovering the password of a non-existing user the POST-request to ”reset-credentials” takes about 20-40 ms. When recovering a password of an existing user this process takes up to ten times longer. This means about 300-500 ms.

Proof of Concept (PoC)

1. Install/Create a new Keycloak instance
2. Set an email adresss on the profile for the user you are using
   - This is needed to test the email connectivity
3. Setup an SMTP-Server, to allow Keycloak sending emails
4. Create a random user
5. Enable password recovery at base configuration
6. Logout and recover password of existing and non-existing user
   - There should be an observable time discrepancy between them

Solution

Disable password recovery via email until this issue was fixed.

Disclosure Timeline

2021-07-12	Vulnerability discovered
2021-08-03	Reported to Red Hat
2021-08-23	No Response from Red Hat, reported again
2021-09-02	Categorized by Red Hat as Security Hardening Issue, no CVE

References

[1] REF Description
https://www.adesso.de

Credits

This security vulnerability was found by Ediz Turcan of adesso SE.
E-Mail: ediz.turcan@adesso.de

Disclaimer

The information provided in this security advisory is provided ”as is” and without warranty of any kind. Details of this security advisory may be updated in order to provide as accurate information as possible. The latest version of this security advisory is available on the adesso SE website.

Copyright