IUCLID 6

Notes on vulnerabilities fixed in version 6.27.6

28/02/2023

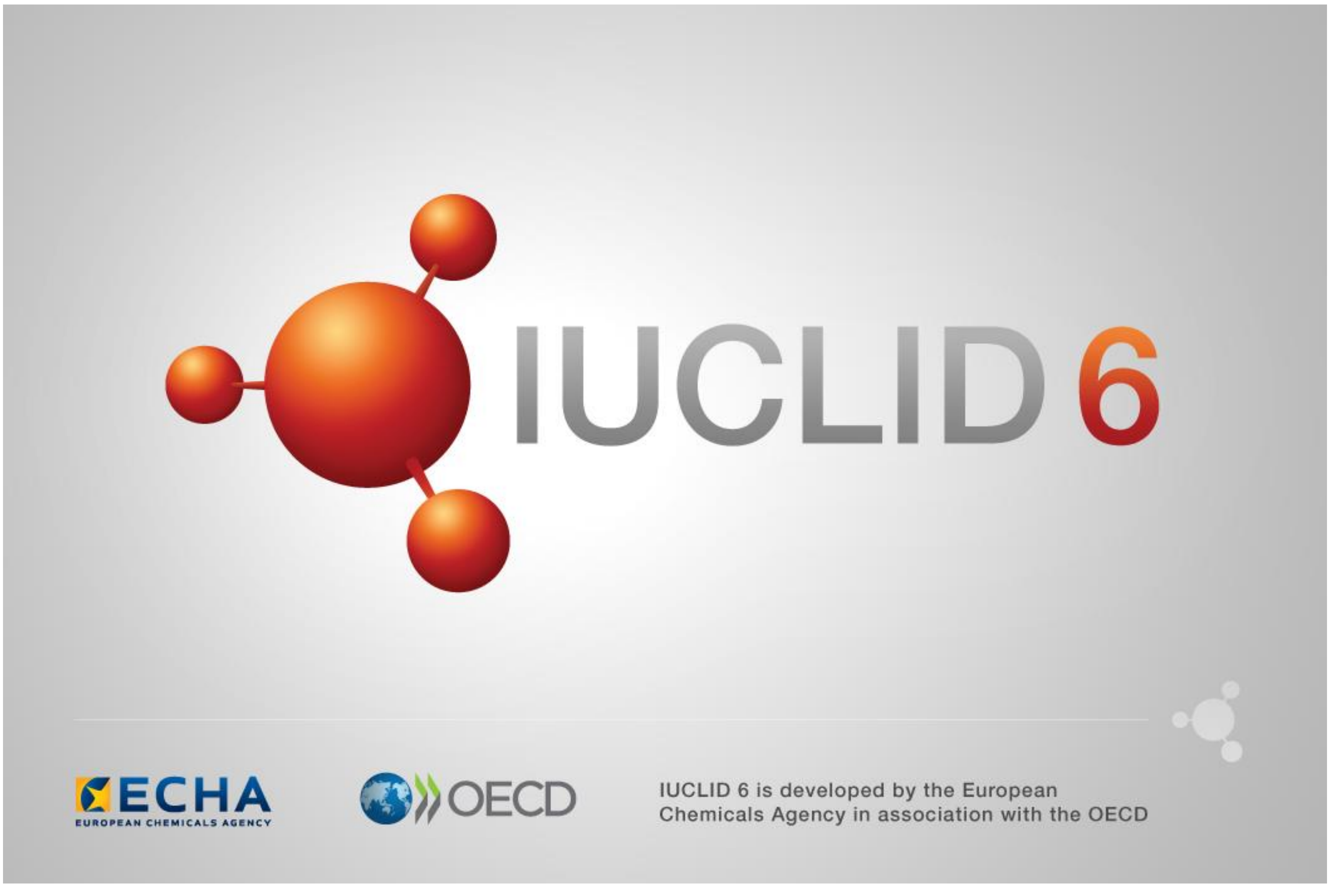
IUCLID 6
ECHA
EUROPEAN CHEMICALS AGENCY
OECD
IUCLID 6 is developed by the European Chemicals Agency in association with the OECD

Table of Contents

1. Introduction

Multiple vulnerabilities in IUCLID 6 application were privately reported to ECHA.
IUCLID 6 version 6.27.6 is available to remediate all these vulnerabilities.

2. Vulnerabilities

2.1. Authentication bypass vulnerability (CVE-2023-26089)

2.1.1. Description

A vulnerability exists in IUCLID 6 application that allows an attacker to bypass the authentication and have an unauthorised access to an IUCLID instance. Because a weak hard coded secret is used to sign the authentication token (JWT), an attacker could have unauthorised access to any affected IUCLID instances as any valid user. The vulnerability can be exploited over network in case the attacker has network access to the IUCLID 6 application.

Please note that versions older than 6.27.1 are also affected even if the hard coded secret in those versions is stronger. The vulnerability has been fixed in version 6.27.6.

2.1.2. Affected versions and severity

IUCLID Version	Severity
IUCLID 6 Server versions 6.27.1 – 6.27.5	**Critical**
IUCLID 6 Server versions 5.15.0 – 6.27.0	High
IUCLID 6 Desktop versions 5.15.0 – 6.27.5	High

2.1.3. Resolution

Update IUCLID to version 6.27.6.

2.1.4. Workarounds and mitigations

1. For versions 6.27.1 – 6.27.5: change the jwt signing secret by executing the following steps on the system where IUCLID 6 is installed
   a. start IUCLID 6
   b. go to the <iuclid6-installation>/payara5/glassfish/bin folder
   c. execute the command: **asadmin update-password-alias iuclid6-idp-secret**
      i. if the command fails with *"Password alias for the alias iuclid6-idp-secret does not exist."* then execute the command: **asadmin create-password-alias iuclid6-idp-secret**
      ii. the command will prompt the user to enter the password twice.
   d. execute the command: **asadmin create-system-properties --target=server-config eu.echa.iuclid6.idp.secret=${ALIAS=iuclid6-idp-secret}**
   e. Restart IUCLID6

2. Limit network access to the IUCLID application. **Particularly, ensure that IUCLID is not available directly from the Internet**. In case a necessary reason to access IUCLID from outside of your internal network exists, then provide such access via VPN or by using another secure remote access solution.

3. Exploitation can be identified by monitoring unusual records in ***audit_iuclid6.log***

and ***user_actions_iuclid6.log*** log files (in <iuclid6-install-folder> \payara5\glassfish\domains\domain1\logs\iuclid6)

2.2. Server-side Template Injection (SSTI) Vulnerability (CVE-2023-26546)

2.2.1. Description

A vulnerability in IUCLID application allows an attacker to execute arbitrary code by uploading a special crafted report template file. The vulnerability can be exploited remotely over network by an authenticated user with template manager permission.

2.2.2. Affected versions and severity

IUCLID Version	Severity
IUCLID 6 Server & Desktop versions 5.15.0 - 6.27.5	**Critical**

2.2.3. Resolution

Update IUCLID to the version 6.27.6.

2.2.4. Workarounds and mitigations

1. Remove the template manager permission from users.

2. Impact of successful exploitation can be mitigated by running IUCLID application with a dedicated operating system account without any unnecessary privileges.

3. Potential exploitation can be identified by checking if any report template file has been uploaded:

   a. The easiest is to check if there are any suspicious custom reports via the IUCLID user interface: Main menu -> Manage Reports
   b. In addition, one could check the user_actions_iuclid6.log (in <iuclid6-install-folder> \payara5\glassfish\domains\domain1\logs\iuclid6) for entries with pattern: “TemplateLoader <report-name> has been registered”

4. Limit network access to IUCLID application. **Particularly, ensure that IUCLID is not available directly from the Internet**. In case a necessary reason to access IUCLID from outside of your internal network exists, then provide such access via VPN or by using another secure remote access solution.

2.3. Cross site scripting (XSS) vulnerability

2.3.1. Description

A reflected XSS vulnerability has been identified in the IUCLID application. The vulnerability allows to run a malicious script on a client device, but exploitation requires user interaction. Thus, an attacker must convince a user to act, typically by clicking a crafted link.

2.3.2. Affected versions and severity

IUCLID Version	Severity
IUCLID Server versions 5.15.0 - 6.27.5	Moderate
IUCLID Desktop versions 5.15.0 - 6.27.5	Low

2.3.3. Resolution

Update IUCLID to the version 6.27.6.

2.3.4. Workarounds and mitigations

There are no known workarounds for this issue.

3. Acknowledgements

ECHA would like to thank Salvatore Bova of Deloitte and Andrea Cecili of Cyber Partners for reporting all three vulnerabilities to us.

4. References

- IUCLID website
  - https://iuclid6.echa.europa.eu/
- IUCLID download page
  - https://iuclid6.echa.europa.eu/download
- Release notes
  - https://iuclid6.echa.europa.eu/documents/1387205/1809509/IUCLID_6_Release_Notes.pdf