National Cyber Security Centre

2202091431-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Alert

Critical Vulnerabilities in SAP Internet Communication Manager (ICM)

2022-02-09

Status: TLP-WHITE

This document is classified using Traffic Light Protocol. Recipients may share TLP-WHITE *information freely, without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.*

Description

SAP have released security updates to address three critical vulnerabilities affecting the Internet Communication Manager (ICM), a core component of SAP business applications. In a collaboration with the SAP Product Security Response Team (PSIRT), Onapsis Research Labs have produced a report on these vulnerabilities which you can download here.

The three vulnerabilities are:

- **CVE-2022-22536** - CVSSv3 - 10.0
  - The most critical vulnerability is a desynchronization of MPI Buffers between the ICM and the backend (Java/ABAP) processes. It is possible to desynchronize the communication between the proxy and the ICM and thereby use HTTP smuggling to hijack a victim's sessions.
- **CVE-2022-22532** - CVSSv3 - 8.1
  - Use After Free in ICM. To exploit this issue, an attacker can send a pipelined request with an incomplete message. The ICM will still get a new MPI Buffer but will stop from parsing the second request. This allows the attacker to write more data that will be placed at the beginning of the new buffer. Thus, a malicious threat actor would be able to take control over the SAP application. However, in this case, it is also possible to write arbitrary responses which could be stored in the internal ICM Web Cache. This means that SAP NetWeaver Java is vulnerable to Arbitrary Web Cache poisoning, which can modify the entire behavior of the application.
- **CVE-2022-22533** - CVSSv3 - 7.5
  - Memory Leak in MPI Management. Using this vulnerability, an attacker can easily consume all MPI resources and cause a denial of service attack in any SAP application exposed through the HTTP(S) port, effectively disrupting business processes and interfaces supported by the application.

Products Affected

- CVE-2022-22536
  - Affecting both stacks and applications behind the SAP Web Dispatcher
- CVE-2022-22532
  - SAP AS Java systems only
- CVE-2022-22533
  - SAP AS Java systems only

Impact

Potential Remote Code Execution (RCE), data theft, operations disruption, ransomware, denial of service.

Recommendations

The NCSC recommends that affected organisations review the Onapsis report and apply the relevant SAP security patches as soon as possible.

Onapsis have created a Python script to check if a SAP system is vulnerable to CVE-2022-22536. You can find the script on their Github page. Please note that this tool cannot guarantee with 100% accuracy whether your SAP applications are vulnerable or not.

DISCLAIMER: *This document is provided "as is" without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.*

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie