# OPC Foundation Security Bulletin

## Security Update for the OPC UA Legacy Java Stack

Published: May 15th, 2023
**Version:** 1.0

## Executive Summary

This security update resolves a vulnerability in the OPC UA Legacy Java Stack that enables an unauthorized attacker to block OPC UA server applications so that they can no longer serve client application.

This security update has a base score of 7.5 (high) using the CVSS v3.1 guidelines.

The CVSS vector string is:
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

## Affected Software

The following software has been updated to address the issue:

| Download | | Replacement |
|---|---|---|
| OPCFoundation/UA-Java-Legacy | | |
| This version or any version after it. | | GitHub Commit: https://github.com/OPCFoundation/UA-Java-Legacy/commit/6f176f2b445a27c157f1a32f225accc9ce8873c0 |

## OPC Foundation Vulnerability Information

Vulnerabilities and Exposures list:

| Vulnerability | CVE number | Publicly disclosed | Exploited |
|---|---|---|---|
| CWE-400 Uncontrolled Resource Consumption. | CVE-2023-32787 | Yes | No |

# Mitigating Factors

None.

# Workarounds

None.

# Acknowledgments

The OPC Foundation recognizes Claroty Team82 Research working with Trend Micro Zero Day Initiative for discovering and reporting this issue.

# Disclaimer

The information provided in this disclosure is provided "as is" without warranty of any kind. OPC Foundation disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall OPC Foundation or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if OPC Foundation or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.

# Revisions

- V1.0 (May 15th, 2023): Bulletin published.