2021-01-05
Version 1.1

Security Advisory WIBU-201218-07

Vulnerability Title

Multiple vulnerabilities in the third-party library XStream, bundled into the AxProtector for Java. No WIBU-SYSTEMS’ products are affected by any of these vulnerabilities.

Vulnerability description

Three vulnerabilities were disclosed for different versions of the third-party library XStream, which is a Java library to serialize objects to XML and back again. These vulnerabilities are related to the manipulation of input streams, which get processed by the XStream library.

The vulnerabilities got assigned the CVE IDs CVE-2020-26217, CVE-2020-26258 and CVE-2020-26259. The CVSS v3.1 base scores are 8.8, 7.7 and 6.8 correspondingly.

Successful exploitation of these vulnerabilities may allow a remote attacker to run arbitrary shell commands, to create Server-Side Forgery Requests or to delete arbitrary files.

XStream comes bundled as part of the AxProtector for Java (AxProtector.jar). The AxProtector for Java is not affected itself by any of these vulnerabilities because a whitelist is used, as recommended in the XStream's Security Framework.

The vulnerabilities CVE-2020-26258 and CVE-2020-26259 don’t exist if running Java 15 or higher.

Affected products and solution

No WIBU-SYSTEMS’ products are affected by any of these vulnerabilities. Nevertheless, the current AxProtector (version 10.70) contains XStream version 1.4.14 to get rid of CVE-2020-26217.

CVE-2020-26258 and CVE-2020-26259 are more recent (first published on 15th December 2020), so the fixed XStream version 1.4.15 will be distributed with the next AxProtector version: 10.70a.

Here is an overview of the CVEs with the affected XStream versions and the corresponding security recommendations:

CVE ID	Affected Product name	Affected XStream versions	Remediation / Recommendations
CVE-2020-26217	No WIBU-SYSTEMS’ products affected	XStream before version 1.4.14	Install the AxProtector version 10.70, which is part of the CodeMeter SDK version 7.20. The XStream library has been updated to a new version without this vulnerability (version 1.4.14).
CVE-2020-26258 and CVE-2020-26259	No WIBU-SYSTEMS’ products affected	XStream before version 1.4.15	Install Java 15 or higher. Install AxProtector version 10.70a (not released yet), which contains an XStream version without these vulnerabilities (version 1.4.15).

Acknowledgments

Internal security tests of WIBU-SYSTEMs discovered that the mentioned vulnerabilities were disclosed for the used versions of XStream.

Disclaimer

The information in this document is subject to change without notice and should not be construed as a commitment by WIBU-SYSTEMS AG. All information that relates to the future (e.g. planned software versions and release dates) is provided without guarantee.

WIBU-SYSTEMS AG provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall WIBU-SYSTEMS AG or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if WIBU-SYSTEMS AG or its suppliers have been advised of the possibility of such damages.

Document History

Version	Date	Description
1.0	2020-12-26	First version
1.1	2021-01-05	Additional details about CVE-2020-26258 and CVE-2020-26259 were added