SECURITY
LICENSING
PERFECTION IN PROTECTION

2021-01-14
Version 1.2

Security Advisory WIBU-201218-07

Vulnerability Title

Multiple vulnerabilities in the third-party library XStream, bundled into AxProtector Java.

Summary

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.

According to the CVEs, 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 AxProtector Java (AxProtector.jar). AxProtector Java is not affected itself by any of these vulnerabilities because a whitelist is used, as recommended in the XStream's Security Framework.

Although AxProtector Java can't be used to exploit these vulnerabilities, a residual risk is still present if an attacker manages to exploit these vulnerabilities in combination with other vulnerabilities, e.g. by finding and executing an existing vulnerable Java application that uses the XStream library on the target system without defining a whitelist. In this case the Java classpath must be configured in a way that the vulnerable Java application ends up using the vulnerable version of XStream bundled into AxProtector Java. Alternatively the attacker could try to take advantage of other vulnerabilities that may exist in the target system to inject a malicious application that uses directly the vulnerable XStream version bundled into AxProtector Java.

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

Affected products and solution

None of these vulnerabilities can be exploited using any WIBU-SYSTEMS AG products. The current AxProtector Java (version 10.70) contains a newer version of XStream (version 1.4.14) to get rid of CVE-2020-26217 on the systems where AxProtector Java is installed.

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 vulnerable XStream versions and the corresponding security recommendations:

CVE ID	Affected Product name	Vulnerable XStream versions	Remediation / Recommendations
CVE-2020-26217	AxProtector Java	XStream before version 1.4.14	Install 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	AxProtector Java	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).

Mitigations for affected versions

Proceed as follows to get rid of these vulnerabilities if an affected version of AxProtector Java was installed but it isn't needed:

- On Linux: delete the file /usr/share/AxProtector/AxProtector.jar
- On macOS: delete the file /Applications/WIBU-SYSTEMS Devkit/AxProtector/AxProtector.jar
- On Windows:
  - If you don't use the AxProtector GUI: delete the file %ProgramFiles(x86)%\WIBU-SYSTEMS\AxProtector\Devkit\bin\AxProtector.jar
  - If you use the AxProtector GUI for encrypting applications other than Java applications: replace the file %ProgramFiles(x86)%\WIBU-SYSTEMS\AxProtector\Devkit\bin\AxProtector.jar with an empty file with the same name. This is needed because the AxProtector GUI verifies whether the file AxProtector.jar is present in this directory.

General security best practices can help to protect systems from local and network attacks.

Vulnerability description

Vulnerability CVE-2020-2621

XStream before version 1.4.14 is vulnerable to Remote Code Execution. The vulnerability may allow a remote attacker to run arbitrary shell commands only by manipulating the processed input stream. Only users who rely on blacklists are affected. Anyone using XStream's Security Framework whitelist is not affected. The issue is fixed in version 1.4.14.

- CVE: CVE-2020-26217
- CVSS v3.1 base score: 8.8
- CVSS v3.1 vector string: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
- Vulnerability type: CWE-78

Vulnerability CVE-2020-26258

XStream is a Java library to serialize objects to XML and back again. In XStream before version 1.4.15, a Server-Side Forgery Request vulnerability can be activated when unmarshalling. The vulnerability may allow a remote attacker to request data from internal resources that are not publicly available only by manipulating the processed input stream. If you rely on XStream's default blacklist of the Security Framework, you will have to use at least version 1.4.15. The reported vulnerability does not exist if running Java 15 or higher. No user is affected who followed the recommendation to setup XStream's Security Framework with a whitelist! Anyone relying on XStream's default blacklist can immediately switch to a whitelist for the allowed types to avoid the vulnerability.

- CVE: CVE-2020-26258
- CVSS v3.1 base score: 7.7
- CVSS v3.1 vector string: AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N
- Vulnerability type: CWE-918

Vulnerability CVE-2020-26259

XStream is a Java library to serialize objects to XML and back again. In XStream before version 1.4.15, is vulnerable to an Arbitrary File Deletion on the local host when unmarshalling. The vulnerability may allow a remote attacker to delete arbitrary files on the host if the executing process has sufficient rights only by manipulating the processed input stream. If you rely on XStream's default blacklist of the Security Framework, you will have to use at least version 1.4.15. The reported vulnerability does not exist running Java 15 or higher. No user is affected, who followed the recommendation to setup XStream's Security Framework with a whitelist! Anyone relying on XStream's default blacklist can immediately switch to a whitelist for the allowed types to avoid the vulnerability.

- CVE: CVE-2020-26259
- CVSS v3.1 base score: 6.8
- CVSS v3.1 vector string: AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:H/A:N
- Vulnerability type: CWE-78

Acknowledgments

Internal security tests of WIBU-SYSTEMS AG 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 internal version.
1.1	2021-01-05	Included additional details about CVE-2020-26258 and CVE-2020-26259.
1.2	2021-01-14	Included additional information about the remaining risk, mitigations and about each vulnerability.