Security Advisory

CVE-2022-23410 - 09.03.2022 (v2.0)

Affected products, solutions, and services

- AXIS IP Utility version 4.17.0 or earlier

Summary

SeungYun Lee from the Korea University in Sejong and James Tsz Ko Yeung from Hong Kong have found flaws in AXIS IP Utility that allows for remote code execution and local privilege escalation by the means of DLL hijacking. IPUtility.exe would attempt to load DLLs from its current working directory which could allow for remote code execution if a compromised DLL would be placed in the same folder.

The vulnerability has been assigned a 7.8 (High) severity by using the CVSSv3.1 scoring system. Learn more about the Common Vulnerability Scoring System here.

Solution & Mitigation

Axis has released a patched version of AXIS IP Utility (version 4.18.0) that adds a verification step when loading DLLs. When unverifiable DLLs are loaded in the working directory, IP Utility will not start, and the user must move the IPUtility.exe into a folder with no DLLs present.

The release notes will state the following:
Extended correction of CVE-2022-23410. For more information, please visit the Axis product security portal.

It is recommended to remove older versions of the AXIS IP Utility and replace it with version 4.18.0 or later. Learn the current version of your AXIS IP Utility by right click on the executable -> Properties -> Details.

The latest AXIS IP Utility can be found here. For further assistance and questions, please contact AXIS Technical Support.

Axis Communications AB, Gränden 1, SE-223 69 Lund, Sweden
Tel: +46 46 272 18 00, Fax: +46 46 13 61 30, www.axis.com