INNEO SECURITY ADVISORY

PATH TRAVERSAL AT STARTUP TOOLS 2018 AND EARLIER

Advisory ID: INNEO-SA-2020-01
Product: Startup TOOLS
Affected Version(s): <= 2018 M040 (13.0.70.3804)
Tested Version: 2018 and earlier
Vulnerability Type: Path Traversal (CWE-22)
Risk Level: Critical
Solution Status: Solved
Solution Date: 2020-07-15

Summary

The Startup TOOLS 2018 and earlier are vulnerable to path traversal attacks which can be eventually leveraged to obtain remote code execution on the target. This vulnerability allows an unauthenticated attacker to read arbitrary files on the server and execute arbitrary code by using logpoisoning.

Note: To exploit this vulnerability, an attacker must be in the corporate network.

This advisory is available at the following link:
https://www.inneo.de/files/content/Produktentwicklung/Tools-und-Erweiterungen/Startup-TOOLS/INNEO-SA-SUT-2020-01.pdf

Solution

INNEO has a newer version 6.x.x.x and ongoing which is the successor of the deprecated versions 2018 and prior. The new version is not prone to this vulnerability anymore as it is a complete redesign of the application itself. INNEO recommends to migrate from the deprecated Startup TOOLS 2018 and prior to at least 6.0.2.0 (recent version by the time of writing) or later.

Source

INNEO would like to thank Patrick Hener, SySS GmbH, for finding and reporting this vulnerability.