Impact of multiple vulnerabilities in Apache Log4j (Log4shell)

Release date: March 29, 2022
Mitsubishi Electric Corporation

■Overview

There are multiple vulnerabilities due to design flaws in Java Logging Framework Apache Log4j. These vulnerabilities could allow an attacker to disclose information, cause a denial-of-service (DoS) or execute malicious programs. The product names affected by these vulnerabilities are shown below, so please implement countermeasures, mitigation measures or workarounds.

■CVSS

CVE-2021-44228(CWE-502):	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	Base Score:10.0
CVE-2021-45046(CWE-502):	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H	Base Score: 9.0
CVE-2021-45105(CWE-20,674):	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H	Base Score: 5.9

■Description

Apache Log4j is vulnerable to information disclosure, denial-of-service (DoS), and remote code execution because it processes and executes log messages without sufficient input validation. Our products may be affected by the following vulnerabilities. Please check the number (from 1 to 3) of vulnerabilities that may be affected for each product in "Affected products countermeasures, mitigation measures, and workarounds".

1. Remote code execution vulnerability due to processing log messages without sufficient validation in JNDI(*) (CVE-2021-44228)(CWE-502)
2. Remote code execution vulnerability under certain conditions due to insufficient fixes for CVE-2021-44228 and processing log messages without sufficient validation in JNDI (CVE-2021-45046)(CWE-502)
3. Denial-of-service(DoS) vulnerability due to insufficient input validation in self-referential Lookup processing and control of improper recursive procrssing. (CVE-2021-45105)(CWE-674、CWE-20)

(*)･･･Java Naming and Directory Interface. An API that provides naming and directory functionality to applications written using the Java programming language.

■Impact

The output of the crafted string by an attacker in some way to a log file can cause information disclosure, a denial-of-service (DoS), or the execution of malicious programs.

■Affected products, countermeasures, and mitigations or workarounds

[1] CC-Link IE TSN Master/Local module Communication LSI (CP610) Setting Tool [CC-Link IE TSN Configurator]

Product Name	Countermeasures and Mitigations/Workarounds
SW1DNN-GN610SRC-M All versions prior to Ver.1.02C may be affected. (Could be affected to 1, 2 and 3.)	<Impact> Exploits to these vulnerabilities against the computer on which this product is installed can result in information disclosure, denial-of-service (DoS), or malicious program execution. <Countermeasures> Download Ver.1.12F or later from below URL, and update the software. https://www.mitsubishielectric.com/fa/#software <How to Update> 1. Unzip the downloaded file (zip format). 2. Please run "SW1DNN-GN610SRC-M.exe" in the extracted folder to install. 3. When you run "Tools.exe" stored in "CCLinkIE_TSN_configuration_tool" folder, "CC-Link IE TSN Configurator" will be expanded in the Tools folder. <Mitigations/Workarounds> If you are unable to update this product immediately, we recommend to take the following mitigation. - When connecting the computer on which this tool is installed to the Internet, use a firewall or virtual private network (VPN) to prevent unauthorized access.

●Contact information

Please contact your local Mitsubishi Electric representative.

<Inquiries | MITSUBISHI ELECTRIC FA>
https://www.mitsubishielectric.com/fa/support/index.html