Multiple Vulnerabilities in web functions of Energy Saving Data Collecting Server (EcoWebServerIII)

Release date: February 15, 2022
Mitsubishi Electric Corporation

■Overview

Multiple vulnerabilities exist in multiple OSS (Open Source Software) installed in Energy Saving Data Collecting Server (EcoWebServerIII). If these vulnerabilities are exploited by a malicious attacker, the information of the product may be disclosed or tampered with, or the product may result in Denial-of-Service (DoS) condition. (CVE-2016-10735, CVE-2017-18214, CVE-2018-14040, CVE-2018-14042, CVE-2018-20676, CVE-2019-8331, CVE-2020-7746, CVE-2020-11022, CVE-2020-11023)

Versions of the Energy Saving Data Collecting Server (EcoWebServerIII) affected by these vulnerabilities are listed below, so please take countermeasures.

■CVSS

- CVE-2016-10735 CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N Base Score:6.1
- CVE-2017-18214 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Base Score:7.5
- CVE-2018-14040 CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N Base Score:6.1
- CVE-2018-14042 CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N Base Score:6.1
- CVE-2018-20676 CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N Base Score:6.1
- CVE-2019-8331 CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N Base Score:6.1
- CVE-2020-7746 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Base Score:7.5
- CVE-2020-11022 CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N Base Score:6.1
- CVE-2020-11023 CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N Base Score:6.1

■Affected products

Affected product model names and versions are listed below.

Product	Model names	Versions
Energy Saving Data Collecting Server (EcoWebServerIII)	MES3-255C-EN	3.0.0 to 3.3.0
	MES3-255C-DM-EN	
	MES3-255C-CN	
	MES3-255C-DM-CN	

The followings are how to check the version.

Please refer to chapter "3.3 How to check the version" on User's Manual (Operating).

*The latest manual is available for downloading on MITSUBISHI ELECTRIC FA Global Website (https://www.mitsubishielectric.com/fa).

■Description

Multiple vulnerabilities due to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (CWE-79) below exist in Energy Saving Data Collecting Server (EcoWebServerIII), which may result in information disclosure or information tampering of the product.

- CVE-2016-10735: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (CWE-79)
- CVE-2018-14040: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (CWE-79)
- CVE-2018-14042: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (CWE-79)
- CVE-2018-20676: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (CWE-79)
- CVE-2019-8331 : Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (CWE-79)
- CVE-2020-11022: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (CWE-79)
- CVE-2020-11023: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (CWE-79)

In addition, multiple vulnerabilities due to Uncontrolled Resource Consumption (CWE-400) and Improperly Controlled Modification of Dynamically-Determined Object Attributes (CWE-915) below exist in Energy Saving Data Collecting Server (EcoWebServerIII), which may result in DoS condition of the product.

- CVE-2017-18214: Uncontrolled Resource Consumption (CWE-400)
- CVE-2020-7746 : Improperly Controlled Modification of Dynamically-Determined Object Attributes (CWE-915)

■Impact

If these vulnerabilities are exploited by a malicious attacker, the information of the product may be disclosed or tampered with, or the product may result in Denial-of-Service (DoS) condition.

■Countermeasures

The followings are fixed versions.

Product	Model names	Versions
Energy Saving Data Collecting Server (EcoWebServerIII)	MES3-255C-EN	3.3.1 or later
	MES3-255C-DM-EN	
	MES3-255C-CN	
	MES3-255C-DM-CN	

For customers who use the affected versions, please refer to the Manual below to update the version.

・Chapter “4.8.6 Version up of Main Program” on User’s Manual (Setting)

＊ The manual and Setting Software for EcoWebServerIII for version up are available for downloading on MITSUBISHI ELECTRIC FA Global Website(https://www.mitsubishielectric.com/fa).

■Mitigation/Workarounds

Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting these vulnerabilities:

- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when Internet access is required.
- Use within a LAN and block access from untrusted networks and hosts through firewalls.

■Contact information

Please contact your local Mitsubishi Electric representative.