MONTELEKTRO

SJEDIŠTE RIJEKA
Kudeji 53
HR-51215 Kastav
rijeka@montelektro.hr
+ 385 51 54 58 10

URED ZAGREB
Marka Marulića 5
HR-10431 Sv. Nedelja
zagreb@montelektro.hr
+ 385 1 39 09 020

SECURITY ADVISORY

CVE-2022-0543 Redis Lua sandbox escape

Revision history:

Date	Rev.	Description
13.12.2023.	1	[DFL] Initial release
01.02.2024.	2	[DFL] Vulnerability confirmed, patch for V990, V980, V970 and V960 released

MONTELEKTRO

TABLE OF CONTENTS

1. INTRODUCTION

A critical vulnerability in Redis (persistent key-value database) identified by CVE-2022-0543 has been publicly disclosed in 2022. Due to the packaging issue, this vulnerability is prone to Debian specific Lua sandbox escape which could result in remote code execution.

On 12th of December 2023. Schneider Electric released Security notification alert stating that this vulnerability is affecting Plant iT products v9.60 and above: *It was discovered, that Redis, a persistent key-value database, due to a packaging issue, is prone to a Lua sandbox escape, which could result in remote code execution. Note: The original CVE description from Redis has been modified in the context of Plant iT.*

ProLeiT Help desk confirmed the Redis database supplied with ProLeiT products can be compromised by this security breach, security update has been developed to rectify the security breach for multiple Plant iT versions. It is strongly recommended to install the security update on the affected computers.

2. PLANT IT PRODUCT EXPOSURE STATUS

2.1. Plant iT V9.90

Cumulative update	Affected	Mitigation
CU2 or later	Yes	Activate secure mode in the system settings
CU1	Yes	Install security update
RTM	Yes	Install security update

Affected computer roles

- Plant iT Server (Standard installation)
- Plant iT Application Server (Enterprise installation)
- Plant iT Visu-Hub
- Plant iT operator station (with direct PLC connection)
- Plant iT Engineering Client (with direct PLC connection)

Unaffected computer roles

- Plant iT operator stations without direct PLC connection
- Plant iT Database Server (Enterprise installation)

Restrictions

If the security update is activated: Only Plant iT Visu-Hubs with connections to all controllers can be used.

Recommendation: Ensure that Visu-Hubs have connections to all controllers.

Alternative: Deactivate Visu-Hubs for which this is not the case.

2.2. Plant iT V9.80

Cumulative update	Affected	Mitigation
CU3.1 or later	Yes	Activate secure mode in the system settings
CU3	Yes	Install security update
CU2	Yes	Install security update
CU1	Yes	Upgrade to CU3.1 and activate secure mode in the system settings
RTM	Yes	Upgrade to CU3.1 and activate secure mode in the system settings

Affected computer roles

- Plant iT Server (Standard installation)
- Plant iT Application Server (Enterprise installation)
- Plant iT Visu-Hub
- Plant iT operator station (with direct PLC connection)
- Plant iT Engineering Client (with direct PLC connection)

Unaffected computer roles

- Plant iT operator stations without direct PLC connection
- Plant iT Database Server (Enterprise installation)

Restrictions

If the security update is activated: Only Plant iT Visu-Hubs with connections to all controllers can be used.

Recommendation: Ensure that Visu-Hubs have connections to all controllers.

Alternative: Deactivate Visu-Hubs for which this is not the case.

2.3. Plant iT V9.70

Cumulative update	Affected	Mitigation
CU4.1 or later	Yes	Activate secure mode in the system settings
CU4	Yes	Install security update
CU3	Yes	Upgrade to CU4.1 and activate secure mode in the system settings
CU2	Yes	Upgrade to CU4.1 and activate secure mode in the system settings
CU1	Yes	Upgrade to CU4.1 and activate secure mode in the system settings
RTM	Yes	Upgrade to CU4.1 and activate secure mode in the system settings

Affected computer roles

- Plant iT Server (Standard installation)
- Plant iT Application Server (Enterprise installation)
- Plant iT Visu-Hub
- Plant iT operator station (with direct PLC connection)
- Plant iT Engineering Client (with direct PLC connection)

Unaffected computer roles

- Plant iT operator stations without direct PLC connection
- Plant iT Database Server (Enterprise installation)

Restrictions

If the security update is activated: Only Plant iT Visu-Hubs with connections to all controllers can be used.

Recommendation: Ensure that Visu-Hubs have connections to all controllers.

Alternative: Deactivate Visu-Hubs for which this is not the case.

2.4. Plant iT V9.60

Cumulative update	Affected	Mitigation
CU5	Yes	Install security update
CU4	Yes	Upgrade to CU5 and activate secure mode in the system settings
CU3	Yes	Upgrade to CU5 and activate secure mode in the system settings
CU2	Yes	Upgrade to CU5 and activate secure mode in the system settings
CU1	Yes	Upgrade to CU5 and activate secure mode in the system settings
RTM	Yes	Upgrade to CU5 and activate secure mode in the system settings

Affected computer roles

- Plant iT Server (Standard installation)
- Plant iT Visu-Hub
- Plant iT operator station
- Plant iT Engineering Client

Unaffected computer roles

- none

Restrictions

If the security update is activated: The automatic update (real-time mode) is deactivated in Operation Manager when searching measured value.

3. MITIGATION RECOMMENDATIONS

As a general security measure, Montelektro strongly recommends protecting network access to devices with appropriate mechanisms.

Patch planning and administration guidelines from Montelektro PCS IT maintenance and security whitepaper should be considered during the patch deployment.

An active SLA contract can be used to check if the system is affected and to support security update planning and deployment on affected components supplied by Montelektro.

4. REFERENCES

Montelektro. (2019, July). *Process Control System – IT maintenance and security Whitepaper*. Retrieved from Montelektro Web site: https://www.montelektro.hr/wp-content/uploads/2022/07/KB1007-Process-Control-System-IT-maintenance-and-security-.pdf

NIST. (2023, November 29). *CVE-2022-0543 Detail*. Retrieved from National Vulnerability Database: https://nvd.nist.gov/vuln/detail/CVE-2022-0543

ProLeiT. (2024, January 23). Security update CVE-2022-0543: Overview information Plant iT V9.60.

ProLeiT. (2024, January 24). Security update CVE-2022-0543: Overview information Plant iT V9.70.

ProLeiT. (2024, January 23). Security update CVE-2022-0543: Overview information Plant iT V9.80.

ProLeiT. (2024, January 23). Security update CVE-2022-0543: Overview information Plant iT V9.90.

Schneider Electric. (2023, December 12). *Security notifications.* Retrieved from Cybersecurity support portal: https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-346-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-346-02.pdf