30. September 2022

SPRECON-V460 SECURITY VULNERABILITY ANNOUNCEMENT 2022-09 ISSUE 1

Log Server, Network password, Database password

PRODUCT MANAGEMENT
Sprecher Automation GmbH
Franckstraße 51, 4020 Linz / Österreich
Tel. +43 732 6908-0
Fax +43 732 6908-278
info@sprecher-automation.com
www.sprecher-automation.com

1. History

Date	Issue	Comment
30.09.2022	1	Created

2. Introduction

Sprecher Automation informs about a report from Copa-Data and Security Researcher Ruben Santamarta detailing a security vulnerability for the SPRECON-V460 Logging Service which is part of the SPRECON-V460 platform standard deployment. Based on this vulnerability additional vulnerabilities concerning “Network Password is encrypted using a reversible algorithm” and “Database Password is encrypted using a reversible key” were discovered. These vulnerabilities affect the default deployment (without proper hardening) of the SPRECON-V460 platform. A successful exploit of the first issue could allow attackers remote access to arbitrary files on a system with a deployment of the SPRECON-V460 platform. Local files containing passwords could be obtained from a remote system. An attack against the hashing and encryption algorithm for the passwords using the additional vulnerabilities may provide additional privileges on the remote system or in the SPRECON-V460 network.

3. Products affected

Systems where the SPRECON-V460 Editor / Engineering Studio, SPRECON-V460 Runtime / Service Engine, SPRECON-V460 Analyzer / Reporting Engine, SPRECON-V460 Web Server / Smart Server, SPRECON-V460 logic Workbench / Logic Studio, or straton Workbench have been installed, by default contain an active SPRECON-V460 Log Server and may be affected by these vulnerabilities.

4. Versions affected

SPRECON-V460 product versions 6.20 up to and including version 10 are affected.

5. Vulnerability details

An attacker who successfully exploits the CVE-2022-34836 vulnerability can remotely access arbitrary files on a system with a deployment of the SPRECON-V460 platform. The risk can be reduced by applying access permissions and restricting the access only to legitimate clients by using the inbound firewall rules on the SPRECON-V460 log service.

An attacker who, in addition to CVE-2022-34836 also successfully exploits CVE 2022-34837, may add additional network clients for a system that has the use of the SPRECON-V460 network enabled for one or more projects and has the SPRECON-V460 network encryption enabled, where no additional network segmentation or firewall rules prevent communication of an arbitrary system to the network server.

A successful exploit may also provide the attacker with the capability to use remote transport from an unauthorized engineering studio for a system that has the SPRECON-V460 network encryption enabled, where no additional network segmentation or firewall rules prevent communication of an arbitrary system to the server with the remote transport server running. An attacker who in addition to CVE-2022-34836 also successfully exploits CVE-2022-34838

on a system with the Editor / Engineering Studio installed, may gain access to parts of the engineering data for projects stored and maintained on this system.

5.1. CVE-2022-34836

SPRECON-V460 log server path traversal vulnerability.

A vulnerability exists in the SPRECON-V460 log server that allow the user read access to arbitrary files on a remote SPRECON-V460 system.

CVSS v3.1 base score and vector:

A CVSS base score of **5.9** has been calculated for this vulnerability.

The corresponding CVSS v3.1 vector:

https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N

5.2. CVE-2022-34837

Network Password is encrypted using a reversible algorithm.

The network password in the initialization file is protected with a reversible algorithm. An attacker may be able to discover the hashing algorithms, encryption algorithms, mechanism and information, that are used to store the network password, allowing to recover the original password.

CVSS v3.1 base score and vector:

A CVSS base score of **6.2** has been calculated for this vulnerability.

The corresponding CVSS v3.1 vector:

https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L

5.3. CVE-2022-34838

Database Password is encrypted using a reversible algorithm.

An attacker may be able to discover encryption algorithms, and information, that are used to store the SQL database password, allowing to recover the original password.

CVSS v3.1 base score and vector:

A CVSS base score of **8.1** has been calculated for this vulnerability.

The corresponding CVSS v3.1 vector:

https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

6. Mitigation

Following workarounds have been evaluated. Although these workarounds will not correct the underlying vulnerability, they block the known attack vectors.

For installations that make use of local logging only: prevent network access to the SPRECON-V460 log server: Block all incoming connections to the SPRECON-V460 log service by changing the inbound firewall exceptions. Update the network configuration for the SPRECON-V460 log service using the startup tool to allow access only for the local host or loopback address and perform a restart of the system.

For installations that act as a central SPRECON-V460 log service: Update the network configuration for the SPRECON-V460 log service using the startup tool and restrict access to the network interface on which the SPRECON-V460 log service must be accessible. Allow only the clients that may connect to the log service via the host machine inbound firewall rules. This will reject arbitrary connections to the log service and allow only configured client hosts or IP address to access the SPRECON-V460 log service.

To limit the read access of arbitrary files by means of the first exploit, a local Windows user can be used to start the logging service, that only has read/write permissions for the LOG folder and read permissions for the zenon6.ini file. This mitigates CVE-2022-34838 but not CVE-2022-34837.

For version 11, making use of the TLS based network encryption instead of the network access based on the symmetric key, mitigates CVE-2022-34837.

It is recommended that the operational environment shall be separated from the SPRECON-V460 Engineering Studio (Operational zoning). This reduces the risk of engineering database access. Limiting engineering database access to the local system only, is a general recommendation from the SPRECON-V460 security guide and mitigates CVE-2022-34838.

7. Patch availability

The Build update mitigating the “CVE-2022-34836 SPRECON-V460 log server path traversal vulnerability”.
For SPRECON-V460 versions 8.20 and 10 Builds 102334 and 102631 respectively.

8. General recommendations

Sprecher Automation generally recommends restricting local physical access to authorized people only.

Sprecher Automation further recommends using application whitelisting to restrict execution of applications to only those applications that are required for the operation of the system.

Sprecher Automation recommends testing the updated version of the SPRECON-V460 software in a test environment to verify normal operation of the system according to project specific configuration and hardware environment, prior to installing the update in a production environment.

Sprecher Automation recommends that a contingency plan is in place to roll back the installation of the update in case of any unexpected issues with the production environment following the installation of the patch.

Sprecher Automation generally recommends keeping the operating system and software up to date.

Sprecher Automation generally recommends using the SPRECON-V460 Engineering Studio on a separate engineering system in a protected environment to which access is restricted to authorized users only and on which appropriate security measures like the use of application whitelisting and antivirus software, are in place.

9. Acknowledgements

Sprecher Automation thanks Copa-Data and Ruben Santamarta for helping to identify the vulnerabilities and in protecting our partners and customers.