SMA Solar Technology AG | Sonnenallee 1 | 34266 Niestetal | Germany
Phone: +49 561 9522-0 | Fax: +49 561 9522-100 | Internet: www.SMA.de | E-mail: info@SMA.de
Amtsgericht (District court) Kassel HRB (registration number) 3972
Vorsitzender des Aufsichtsrats (Chairman of the Supervisory Board): Uwe Kleinkauf
Vorstand (Managing Board): Ulrich Hadding, Dr.-Ing. Jürgen Reinert

Manufacturer's declaration

INFORMATION ON VULNERABILITY - Log4S or Log4Shell vulnerability in the Java library Log4j

Description:	Log4S or Log4Shell vulnerability in the Java library Log4j
Affected versions:	Log4j version numbers >= 2.0 and <= 2.14.1
CVE number:	CVE-2021-44228 (https://nvd.nist.gov/vuln/detail/CVE-2021-44228)
Criticality (CVSS 3.1 score)	10.0
Date of release:	2021-12-10

Description of the vulnerability

Log4j is a commonly used logging library for Java applications. It is used for high-performance aggregation of an application's log data. Via a vulnerability named "Log4S" / "Log4Shell" (CVE-2021-44228), attackers may be able to execute their own program code on the target system and compromise it.
Some SMA products also use this library. However, according to current knowledge, SMA inverters are not affected by this vulnerability.

Affected SMA products

Firmware updates that counter the Log4Shell vulnerability are available for the following products. The updates have already been installed to the devices if automatic updates are enabled:

- Data Manager M, Data Manager M Lite (EDMM-10, EDMM-US-10, EDMM-10.A)
  Vulnerability is fixed with firmware version greater than or equal to 1.13.22.R
- SMA EV Charger 7.4/22
  Vulnerability is fixed with firmware version greater than or equal to 1.1.35.R
- Data Manager L (EDML-10)
  Current firmware version on request
- Power Plant Manager, component EDML-10
  Current firmware version on request

A risk assessment was carried out for the subsequent PC-based software applications and the risk was classified as very low, provided that the PC-based software applications are used as intended and thus cannot be accessed or controlled directly via WAN or Internet. There are currently no updates available.

- Sunny Home Manager Assistant
- SMA Connection Assistant

All other SMA products** not listed in this document are **not affected!

Immediate actions

If

- Your device is affected by the Log4Shell vulnerability (see above),
- contrary to our recommendations, your SMA device can be accessed remotely, i.e., directly from the Internet, without additional protective measures (e.g. by so-called port forwarding),
- and as long as this device is not at the current update level yet (see "Affected SMA products")

we urgently recommend that you immediately take the following measures:

- (Default setting recommended by SMA) Activate the automatic update feature so that your device can receive any necessary updates immediately, and also in the future.
- Switch off port forwarding in your router.
- If, however, you have not activated any automatic updates,
  - temporarily disconnect the network connection to the WAN/Internet, e.g., by setting up appropriate access restrictions in your firewall and/or segmenting the network where the affected device is located.
  - Perform the necessary update manually as soon as it is available.
- Activate logging of incoming and outgoing network traffic in your router and periodically review the log data.
- Restrict outgoing connections of the affected device in your router.

Provision of software updates

SMA has already created software updates for the affected products to resolve this vulnerability and made them available for download. Devices configured for automatic updates have already been updated to the necessary firmware version. Please check the firmware status of your device.
If the strongly recommended automatic update is not possible for technical reasons, the necessary update must be performed manually for affected devices. Contact the SMA Service Line.

Niestetal, 2022-01-17
SMA Solar Technology AG

i.V. Sven Bremicker
Head of Technology Development Center