WHITEPAPER CYBER SECURITY

STATEMENT BY SMA SOLAR TECHNOLOGY AG ON THE CYBER SECURITY OF PV INVERTERS (HORUS SCENARIO)

In a presentation at the SHA2017 security conference and on a separate website https://www.horusscenario.com, the Dutch security engineer Willem Westerhof has described the scenario of a Europe-wide blackout. This scenario is based on a hypothetical, large-scale cyberattack on inverters in PV systems. He supports this scenario with a vulnerability analysis of two SMA solar inverters of the same model developed eight years ago. The analysis was conducted for a thesis together with the Dutch security company ITSec.

We appreciate such activities and analysis because they help continuously improve safety standards, which constantly change due to fast technical progress. When looking more closely and competently, however, this scenario is based on a dubious mixture of facts, wavering generalization and inaccurate conclusions. In addition, the deficiency analysis conducted inadequately considers the complex structure and technical standard of inverters. We therefore think it is necessary to explain our perspective and to go into the detail regarding the security issues of the older devices mentioned by Willem Westerhof.

Correction of false statements – here are some key facts:

- From our extensive product portfolio, only the following SMA inverter types are affected: Sunny Boy models TLST-21 and TL-21, Sunny Tripower models TL-10 and TL-30.
- All other products comply with the latest security standards for defending against cyber attacks.
- The attack scenario described for the inverters mentioned above requires extremely high efforts and extensive expertise by a potential hacker.
- Even the devices mentioned above are properly protected from hacker attacks, if the users carefully adhere to the measures outlined in our public cyber security guidelines.
- Any device not connected to the internet is not affected.
- There also is no such thing as a "secret super password" as the author states elsewhere. Our inverters are delivered to our customers with a default password and we actively ask our customers to change this password to a personal secure password immediately after installation.

- Regarding possible effects on the public power supply, Willem mentions 17 GW of solar inverter power sold to the private market by SMA. This is the whole inverter power SMA has sold so far to the residential market. The power produced with the inverters that might be vulnerable to an attack is only a small fraction of this, and they are installed all over the world. So we see absolutely no danger to grid stability even in the extremely unlikely event that all inverters should be successfully attacked at the same time.

Our full statement:

Westerhof performed his analysis on an existing facility equipped with two three-phase Sunny Tripower inverters with a local network connection to which he had direct access. The communication architecture of solar inverters is designed to be installed behind a router with a firewall (such as a DSL router). This is usually the case for all households, whereby the security depends on the router configuration and equipment. As a manufacturer of inverters, we have little influence on these aspects. Certainly, we like to provide support to our customers in implementing a secure configuration.
The inverter itself therefore consciously does not have its own firewall functionality and does not use encrypted communication within the protected local area network, which is currently the state of the art in most home networks. By contrast, the WebConnect standard used outside the closed network generally uses encryption. Most of the attacks described by Willem Westerhof are only possible if the attacker is already INSIDE the local network, i.e., he would first have to have hacked/bypassed the various routers/firewalls of PV system owners to a considerable extent. Otherwise, a brute-force attack, for example, on an inverter login or the changing of the inverter's settings as he describes it is not possible. Given the variety of router systems, this is very difficult to automate (or to automate well), and therefore of only limited suitability for a comprehensive hacker attack. This fact is entirely missing in Westerhof's scenario for reasons that are sadly not clear to us.
The same goes for the larger string inverters used at industrial plants or to supply supermarkets. These are usually protected by firewalls run by a professionally managed IT infrastructure. Large-scale inverters in solar power plants, which incidentally make up most of the total installed gigawatt capacity, are not usually accessible on the Internet, and are instead connected to a control center via secure connections.

Decentralization of production makes cyberattacks more difficult

Modern SMA equipment families have highly developed security architectures and completely different access mechanisms that take into account the sharp increase in security requirements in recent years. In our opinion, there is therefore little merit to conclusions about the vulnerability of all PV inverters available on the market drawn from specific vulnerabilities of older equipment families. Only a small share of PV inverters is connected to the Internet. They account for only around 25% worldwide of the 17 GW mentioned by Westerhof, i.e. just 4 GW. Therefore, given an average system size of 4 kW in a private household, roughly one million routers in private households would have to be hacked and brought under control to achieve a scale relevant to the power grid. Distributed regenerative power generation is therefore also an advantage in this respect and not a disadvantage. Decentralized production and the plurality of inverter families and manufacturers mean that an attack requires a much higher quantitative effort than for central production. Even the massive use of bots would be of very limited help as each system would require an individually configured attack profile.

We have also performed and published a detailed analysis of the vulnerabilities presented by Willem Westerhof. Our own assessment of criticality differs substantially from Willem Westerhof's. Two specific examples:
Willem Westerhof claims that it would have been possible for him to successfully install manipulated firmware on the inverter. This is not correct – while the Sunny Explorer software shows him that the transfer was successful (which he calls "successful flashing"), the new binary is not actually installed as it is partially encrypted and must successfully go through further integrity tests. This is a procedure that is conducted by the device's internal installation routine after the upload.
Willem Westerhof also claims that the devices run a Linux operating system and are therefore exposed to typical Linux vulnerabilities. Having established this, he speculates in his presentation that there is a master password for all devices that would allow universal access. He is wrong on both counts. The device he looked at has no operating system in the usual sense, and there is no master password that would grant user or other rights for any of our inverters. Further errors in the interpretation of the vulnerabilities can be found in our detailed analysis of the CVEs.

Compliance with guidelines minimizes the risk of successful cyberattacks

Three identified vulnerabilities (limiting the choice of password, the mandatory changing of initial default passwords and an additional mechanism for preventing brute-force attacks for guessing passwords) are currently being resolved in a security update we are planning for the product families affected. However, we do not think these as serious as Westerhof claims when SMA's IT security guidelines (http://files.sma.de/dl/7680/CyberSecurity-TI-en-10.pdf) are complied with in installations.

Another scenario—of denial-of-service attacks—only has minimal effects in reality. In principle, denial-of-service attacks are difficult to prevent or can only be prevented with extremely high effort. However, they can only disrupt the transfer of data to the Internet by the affected devices; at worst, the communication module of the inverters affected will stop responding. The inverters' actual operating communication software is not affected, firstly because it runs independently of the module and secondly because multiple (redundant) channels are used in many respects. This is already a requirement of the grid connection guidelines, the professional association and UL (Underwriter Laboratories, USA). It therefore does not affect the power feed.

A Horus scenario, i.e. that a large number of inverters are suddenly and deliberately shut down as a result of a cyberattack, is extremely unlikely

As stated above, Willem Westerhof's Horus scenario makes generalizations about an entire portfolio based on the vulnerabilities of individual devices. The vulnerabilities presented in his analysis are not enough to produce the kill chain he describes, and the author has not yet provided evidence for this either in his presentation or on his website. Furthermore, far fewer inverters can be accessed via an Internet interface – the real plurality of equipment, manufacturers and security mechanisms makes such an attack extremely complex. Given this, we consider the actual probability of a successful attack to be low. Additionally, we are not aware of any evidence that SMA PV inverters have been influenced by unauthorized third parties in real operation.
The fact is, however, that the rising share of solar energy in regenerative energy generation is increasing the relevance of this kind of power generation to the system. There will never be absolute security, as is shown by numerous examples in other sensitive industries. SMA responds to this by constantly evolving its security measures. Without exception, all new communication mechanisms are subjected to testing by external security firms and there are regular audits of our security, IT and portal infrastructure. We are constantly working on new security concepts and have a wide range of committees and partners serving this purpose.
Nobody can completely rule out a "Horus" scenario such as this, but we stake our brand on making it as unlikely as possible.

Comments on CVEs:

We would like to comment on the specific vulnerabilities cited on the website https://horusscenario.com/CVE-Information/ in detail below. For reasons of clarity, only excerpts from the texts on the CVEs (common vulnerabilities and exposures) are shown here. We have added our own assessment to the criticality assessment (CVSS vectors) as regards the mass manipulation of inverters (using the usual scale of 0 to 10, from non-critical to critical).

Please note again that the introduction frequently used in the CVE texts *"An issue was discovered in SMA Solar Technology products"* always relates only to a handful of older model series. The devices of the current development generation have a completely different operating system and a configuration and control environment that has been significantly advanced in terms of its security technology.

CVE-2017-9851

[Suggested description]
An issue was discovered in SMA Solar Technology products. By sending nonsense data or setting up a telnet session to the database port of the Sunny Explorer, the application can be crashed.

Even if this is exploited, there is no further damage beyond a communication failure. The inverter still works as before, only Sunny Explorer (the program that does not run on the inverter and is used to start or service it) has to be restarted. A telnet attack behind the firewall of the home network is only possible, if the router's firewall was previously manipulated or the router's security rules were abrogated. Communication between the Sunny Explorer application and the inverter is not possible outside the local network.

[Additional Information]
CVSS vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L (4.0)

SMA rating:
CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:N (0.0)

CVE-2017-9852

[Suggested description]
An issue was discovered in SMA Solar Technology products. Default passwords exist which are rarely changed. User passwords will almost always be 0000. Installer passwords are expected to be default or similar across installations installed by the same company. Hidden user accounts have (at least in some cases, though more research is required to test this for all hidden user accounts) a fixed password for all SMA devices. This allows passwords to be easily guessed or predicted, compromising the affected device and its functions.

Default passwords for user and installer are reused across inverters. Installer passwords are sometimes changed, but are expected (based on field tests) to be the same across installations installed by the installer company. This enables an attacker to simply guess passwords that are used a lot. It also ensures that if one system is compromised, multiple systems are compromised.

It is the responsibility of the system operator/installer to assign passwords with a minimum level of complexity. As the manufacturer, we state this clearly both in our documentation and our security guidelines. We have no influence on the allocation of passwords, and we neither wish nor are able to check passwords.

Default passwords for user and installer are reused across inverters. Installers' passwords are sometimes changed, but are expected to be the same across installations installed by the installer company.

This is in fact a practice we have observed among companies that install and monitor systems (for convenience). We explicitly state in our security policy that this practice should be stopped.

Every Grid Guard code however, can be used on every SMA inverter. There are also hidden user accounts of which the password can never be changed by the user. An attacker with access to such a password can use this password on any SMA inverter with success. Other vulnerabilities exist that allow an attacker to get the passwords of these hidden user accounts. This ensures that if one system can be compromised, all systems can be compromised.

The author seems to have fundamentally misunderstood how GridGuard-Code works. GridGuard-Code is NOT a security feature per se, it is a way of making it possible to trace changes to network settings. The code assigned for this is therefore assigned to a person and not the inverter, and SMA registers the identity of the person to whom the code is assigned. It is therefore a kind of electronic identity whose activity is noted, e.g., in the inverter log. The GridGuard-Code code can only be used in conjunction with the device's (individually set) installer password; it cannot be used solely to login to the device.

Otherwise the GridGuard-Code code is usually only used for start-up, and even then only as an exception.

In actual fact, in addition to installer and operator accounts there are also service and developer accounts that are used, for example, for repairs and servicing (so that users or installers do not have to compromise their personal passwords when they send the device in for repair or SMA comes round to service it). These accounts are purely for a deeper diagnosis of the device and also have secure passwords specific to the device. They are used exclusively by SMA personnel and also only if the system operator/owner expressly gives SMA Service permission to do so.

Contrary to Westerhof's claims, global hardcoded master passwords do NOT exist.

[Additional Information]
CVSS vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H (8.1)

SMA rating: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:L/A:L (5.8)

CVE-2017-9853

[Suggested description]
An issue was discovered in SMA Solar Technology products. All SMA inverters have a very weak password policy regarding the user and installer password. Many characters cannot be used; no complexity requirements or length requirements are set. Specifically, complex passwords are even impossible due to a maximum of 12 characters and a limited set of characters.

This complexity was the state of the art at the time the inverters in question were developed. A 12-character, case-sensitive password consisting of letters, numbers and common special characters is already a very high security standard. Also, exotic special characters are rarely used in practice in our experience.

Nevertheless, SMA will soon be releasing a firmware update for the devices that allows random passwords, forces the changing of initial default passwords and provides protection against brute-force password attacks.

Other "hidden" user accounts have a
password which is impossible to change for regular users.

See comment on CVE-2017-9852.

[Additional Information]
CVSS vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:N (0.0)

SMA rating: same

CVE-2017-9854

[Suggested description]
An issue was discovered in SMA Solar Technology products. By sniffing for specific packets on the localhost, plaintext passwords can be obtained as they are typed into the Sunny Explorer by the user. These passwords can then be used to compromise the overall device.

This means "sniffing" an internal Sunny Explorer session. Naturally this requires that this tool (which is purely a start-up and service tool) performs the activity the hacker wants at the precise moment of sniffing. The actual likelihood of this is low as it is usually activated only once during the installation.

[Additional Information]
One of the CVE's that could potentially be used in the Horus scenario.
CVSS vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:L/I:N/A:N (3.6)

SMA rating: CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N (2.7)

CVE-2017-9855

[Suggested description]
An issue was discovered in SMA Solar Technology products. A secondary authentication is available for Installers called the grid guard system. This system uses predictable codes, and a single Grid guard code can be used on any SMA inverter. Any such code, when combined with the installer account, allows changing very sensitive parameters.

See comment on CVE-9852 (double).

[Additional Information]
CVSS vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H (8.1)

SMA rating: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:U/C:L/I:H/A:L (5.2)

CVE-2017-9856

[Suggested description]
An issue was discovered in SMA Solar Technology products. Sniffed passwords from SMAdata2+ communication can be decrypted very easily. The passwords are encrypted using a very simple encryption algorithm. This enables an attacker to find the plaintext passwords and authenticate to the device. For this CVE too, an already hacked local network is a prerequisite. In addition, this kind of authentication during start-up using Sunny Explorer usually only takes place once.

[Additional Information]
One of the CVE's that could potentially be used in the Horus scenario.
CVSS vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N (3.4)

SMA rating:
CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N (2.7)

CVE-2017-9857

[Suggested description]
An issue was discovered in SMA Solar Technology products. The SMAdata2+ communication protocol is vulnerable to man in the middle, packet injection, and replay attacks. Any setting change, authentication packet, scouting packet etc. can be replayed, injected, or used for a man in the middle session. All functionalities available in Sunny Explorer can effectively be done from anywhere within the network as long as an attacker gets the packet setup correctly. This includes the authentication process for all (including hidden) access levels and the changing of settings in accordance with the gained access rights.

The SMAdata2+ communication channel is unencrypted. An attacker capable of understanding the protocol can eavesdrop on these communications. Sensitive data should not be transmitted using this protocol. Any sensitive data transmitted over this channel can be retrieved by a malicious hacker by packet sniffing. For example, passwords can be extracted from the network communications this way. These passwords can then be used to compromise the overall device.

This is a general state of the art for a separate subnetwork, including in the energy sector or the smart home sector. Otherwise protocols such as Modbus/TCP, IEC60870 and IEC61850 are used in this environment, which also transmit data without encryption. It is therefore not a vulnerability specific to SMA. To establish a basic security in this respect, we ask our customers to adhere to our guidelines (http://files.sma.de/dl/7680/CyberSecurity-TI-en-10.pdf).

[Additional Information]
This CVE can be used as part of the Horus scenario.
CVSS vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H (8.1)

SMA rating: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:L (4.3)

CVE-2017-9858

[Suggested description]
An issue was discovered in SMA Solar Technology products. By sending crafted packets to the SMA inverter and observing the response, active and inactive user accounts can be determined. Based on the responses, several hidden accounts exist. This aids in further attacks (such as a brute-force attack) as one now knows exactly which users exist and which do not.

See CVE-2017-9852. The existence of additional accounts is not a security gap per se, as long as they are protected with secure passwords specific to the device. Diagnostic access is the state of the art for all technical systems that can be configured by software, and it is not insecure by default.

[Additional Information]
This CVE can be used as part of the Horus scenario.
CVSS vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N (4.0)

SMA rating:
CVSS:3.0/AV:A/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N (2.9)

CVE-2017-9859

[Suggested description]
An issue was discovered in SMA Solar Technology products. The inverters make use of a weak hashing algorithm to encrypt the password for REGISTER requests. This hashing algorithm can be cracked relatively easily. An attacker will likely be able to crack the password using offline crackers. This cracked password can then be used to register at the SMA servers.

It would theoretically be possible to crack the REGISTER request. However, you also need a combination of PIC (product identification code) and RID (registration identification) that is different from the PIC and RID already assigned, and that must be considered valid by the SMA registration server. The user data communication allowed after successful registration does not use a SIP protocol and is also SHA-256 encrypted according to the current state of the art. In practice, we consider the probability of the success of such manipulation to be extremely low.

[Additional Information]
This CVE can be used as part of the Horus scenario.
CVSS vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N (4.0)

SMA rating:
CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:C/C:N/I:N/A:N (0.0)

CVE-2017-9860

[Suggested description]
An issue was discovered in SMA Solar Technology products. An attacker can use Sunny Explorer or the SMAdata2+ network protocol to update the device firmware without ever having to authenticate. If an attacker is able to create a custom firmware version which is accepted by the inverter, the inverter is compromised completely. This allows the attacker to do nearly anything: for example, giving access to the local OS, creating a botnet, using the SMA inverters as a stepping stone into companies etc. The device can be completely compromised this way.

This is a claim that is simply not correct. Westerhof is obviously not familiar with the measures necessary for a firmware update; he also has no proof that the update described was successfully carried out. Sunny Explorer may have given the impression that the action described was successful, but in fact it merely reported that the file was transferred in full. A final integrity and compatibility check is carried out by the installation routine on the inverter using a complex procedure only after transmission.

[Additional Information]
This CVE can be used as part of the Horus scenario.
CVSS vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H (8.1)

SMA rating:
CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:U/C:L/I:L/A:L (3.9)

CVE-2017-9861

[Suggested description]
An issue was discovered in SMA Solar Technology products. The used SIP implementation is vulnerable to replay attacks, packet injection attacks and man in the middle attacks. An attacker is able to successfully use SIP to communicate with the device from anywhere within the LAN. An attacker may use this to crash the device, stop it from communicating with the SMA servers, exploit known SIP vulnerabilities, or find sensitive information from the SIP communications.

The SIP communication channel is unencrypted. An attacker capable of understanding the protocol can eavesdrop on these communications. Sensitive data should not be transmitted using this protocol. All communications should be considered readable for attackers. Sensitive data transmitted over this channel can be retrieved by a malicious hacker. For example, passwords can be extracted from the network communications this way.

See comment on CVE 2017-9859.

[Additional Information]
This CVE can be used as part of the Horus scenario.
CVSS vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:H/A:H (8.9)

SMA rating: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:N/I:N/A:N (0.0)

CVE-2017-9862

[Suggested description]
An issue was discovered in SMA Solar Technology products. When signed in to the Sunny Explorer with a wrong password, it is possible to create a debug report, disclosing information regarding the application and allowing the attacker to create and save a .txt file with contents to his liking. An attacker may use this for information disclosure, or to write a file to normally unavailable locations on the local system where the Sunny Explorer is allowed.

This is possible in principle, but the information contained in the debug report is of marginal significance to a hacker, e.g., no user or password information. Both sides consider this non-critical.

[Additional Information]
This CVE can be used as part of the Horus scenario.
CVSS vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N (0.0)

SMA rating: same

CVE-2017-9863

[Suggested description]
An issue was discovered in SMA Solar Technology products. If a user simultaneously has Sunny Explorer running and visits a malicious host, cross-site request forgery can be used to change settings in the inverters. For example, issuing a post request to change the user password, etc. All Sunny Explorer settings available to the authenticated user are also available to the attacker. (In some cases, this also includes changing settings that the user has no access to.) This may result in complete compromise of the device.

This is highly unlikely in practice because it can only work if Sunny Explorer is used for service/start-up at the same time AND a malicious host is contacted at the same time AND this host is also specifically set up to manipulate the settings of these specific devices.

[Additional Information]
This CVE can be used as part of the Horus scenario.
CVSS vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H (8.3)

SMA rating: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:L/A:L (5.8)

CVE-2017-9864

[Suggested description]
An issue was discovered in SMA Solar Technology products. An attacker can change the plant time even when he is not authenticated in any way. This changes the system time, possibly affecting lockout policies, random generators based on time stamps, and makes timestamp for data analysis unreliable.

The time stamp is only used in the devices to note the time of log entries. The benefit a hacker can gain from this is absolutely marginal. The devices do not use lockout policies or random generators based on time stamps. This is pure speculation on the part of Westerhof. In addition, when online, the system time is synchronized with a valid NTP time again a short time later (when an authorized user logs in at the latest).

[Additional Information]
This CVE can be used as part of the Horus scenario.
CVSS vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N (3.7)

SMA rating:
CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:N (0.0)

Conclusion:

Westerhof classifies two of the 14 vulnerabilities mentioned (9853 and 9862) as absolutely uncritical. The three scenarios 9863, 9859 and 9854 described are extremely unlikely or based on events, which only occur once when installing the plant, and are therefore absolutely unsuitable for access due to a large-scale attack. Two others are based on incorrect perceptions: 9860 that successful firmware update possible without authentication; and 9861 that the SIP protocol is not used for data transfer and instead only for establishing a connection. Two others, 9857 and 9858 describe an absolutely usual state of the art. Even if a commissioning program crashes without further consequences (9851) is not an argument for a kill chain. We think that, from a present-day perspective, the outdated password architecture (missing enforcement for a default password change and limitations regarding password characters and length) and a missing barrier for brute-force attacks on the password essentially remain. However, when installed properly within a closed network according to our cyber security guidelines with an adequate password set, will result in a secure system. Nevertheless, we will soon provide a firmware update for the four device families to address this issue.

Please contact us if you have any further questions on the safety of our products.