WHITEPAPER CYBER SECURITY

STELLUNGNAHME SMA SOLAR TECHNOLOGY AG ZUR CYBER SECURITY BEI PV-WECHSELRICHTERN (HORUS-SZENARIO)

Im Rahmen eines Vortrags auf der Sicherheitskonferenz SHA2017 sowie einer eigenen Webseite https://www.horusscenario.com beschreibt der niederländische Sicherheits-Ingenieur Willem Westerhof das Szenario eines europäischen Strom-Blackouts. Basis dieses Szenarios ist ein hypothetischer großangelegter Cyberangriff auf Wechselrichter in Solaranlagen. Er untermauert dieses Szenario mit einer Schwachstellenanalyse zweier vor acht Jahren entwickelten SMA Solarwechselrichter des gleichen Modelltyps. Durchgeführt wurde die Analyse im Rahmen einer Hochschulabschlussarbeit gemeinsam mit der niederländischen Sicherheitsfirma ITSec.

Wir begrüßen solche Aktivitäten und Analysen grundsätzlich, denn sie unterstützen die kontinuierliche Verbesserung von Sicherheitsstandards, die sich aufgrund des schnellen technischen Fortschritts permanent weiterentwickeln. Bei näherer und sachkundiger Betrachtung beruht dieses Szenario aber auf einer fragwürdigen Mischung aus Fakten, unschlüssigen Verallgemeinerungen sowie unzutreffenden Schlussfolgerungen. Die durchgeführte Schwachstellenanalyse berücksichtigt zudem den komplexen Aufbau und den Stand der Technik bei Wechselrichtern nur unzureichend. Wir sehen es daher als notwendig an, unsere Sicht des Szenarios zu erläutern und im Detail auf die von Willem Westerhof angeführten Sicherheitslücken dieser älteren Gerätefamilien einzugehen.

Richtigstellung der Falschaussagen – hier die Fakten auf einen Blick:

- Aus dem SMA Portfolio sind die Modellreihen Sunny Boy TLST-21 und TL21 sowie Sunny Tripower TL-10 und TL-30 betroffen.
- Alle anderen Produkte entsprechen den neuesten Sicherheitsstandards gegen Cyber-Angriffe.
- Das in dem Artikel beschriebene Szenario eines Angriffs bei diesen Geräten ist hoch komplex und erfordert erhebliche Erfahrung eines potenziellen Hackers.
- Auch die genannten Geräte weisen einen umfassenden Schutz vor möglichen Hacker-Attacken aus, wenn die Maßnahmen unserer veröffentlichten Cyber Security-Richtlinien sorgfältig eingehalten werden.
- Alle Geräte, die nicht mit dem Internet verbunden sind, sind auch nicht direkt betroffen.
- Es gibt darüber hinaus kein „geheimes Super-Passwort“, wie der Autor an anderer Stelle behauptet. Unsere Wechselrichter werden mit einem voreingestellten Passwort ausgeliefert, welches auf unseren ausdrücklichen Hinweis vom Anwender nach der Installation zurückgesetzt und geändert werden sollte.

- Bezüglich möglicher Auswirkungen auf das öffentliche Stromnetz wird in dem Artikel die Aussage getroffen, dass SMA 17 GW Wechselrichterleistung im privaten Hausanlagen-Segment verkauft habe. Dies ist aber die gesamte Wechselrichter-Leistung, die SMA in diesem Segment auf den Markt gebracht hat. Die Leistung, die von den betroffenen Geräten produziert wird, betrifft hiervon nur einen Bruchteil. Darüber hinaus sind die Wechselrichter weltweit installiert. Daher sehen wir in keiner Weise das Risiko möglicher Instabilitäten bezüglich des öffentlichen Netzes, selbst im höchst unwahrscheinlichen Fall einer zeitgleichen Attacke der betroffenen Geräte.

Unsere Stellungnahme im Detail:

Herr Westerhof führte seine Analyse in einer Bestandsanlage durch, ausgestattet mit zwei dreiphasigen Sunny Tripower-Wechselrichtern mit lokaler Netzwerkanbindung, auf welche er direkten Zugriff hatte. Die Kommunikations-Architektur von Solar-Wechselrichtern ist dafür ausgelegt, dass diese hinter einem Router mit Firewall (also z.B. einem DSL-Router) installiert werden. Dies ist bei allen Haushalten üblicherweise der Fall, wobei die Sicherheit von der Konfiguration und dem Equipment des Routers abhängt. Auf diese haben wir als Wechselrichter-Hersteller wenig Einfluss. Wir unterstützen unsere Kunden allerdings gerne bei einer sicheren Konfiguration.

Der Wechselrichter selbst besitzt daher bewusst keine eigene Firewall-Funktionalität und kommuniziert innerhalb des abgeschotteten lokalen Netzwerks nicht verschlüsselt, was derzeit in den meisten Heim-Netzwerken gelebter Stand der Technik ist. Das außerhalb des geschlossenen Netzwerks zum Einsatz kommende WebConnect-Protokoll verwendet dagegen generell eine Verschlüsselung. Die meisten der von Willem Westerhof geschilderten Attacken sind nur möglich, wenn sich der Angreifer bereits INNERHALB des lokalen Netzwerks befindet, d.h. er müsste vorher in erheblichem Umfang die unterschiedlichsten Router/Firewalls von Solaranlagen-Besitzern gehackt/überwunden haben. Anders ist z.B. eine dort geschilderte Brute-Force-Attacke auf einen Wechselrichter-Login oder eine Parameter-Verstellung im Wechselrichter nicht möglich. Dies ist aufgrund der Vielfalt von Router-Systemen sehr schwierig und schlecht automatisierbar, daher für einen größeren Hackerangriff nur sehr bedingt geeignet. Dieses Faktum fehlt im Westerhof'schen Szenario aus für uns nicht nachvollziehbaren Gründen leider gänzlich.
Gleiches gilt auch für die größeren String-Wechselrichter, die auf Industrieanlagen oder zur Versorgung von Supermärkten eingesetzt werden. Auch diese befinden sich üblicherweise hinter Firewalls einer professionell verwalteten IT-Infrastruktur. Großwechselrichter in Solarkraftwerken, die im Übrigen den Großteil der insgesamt installierten Gigawatt-Kapazität ausmachen, sind industrieüblich nicht über das Internet erreichbar, sondern über gesicherte Verbindungen mit einer Leitstelle verbunden.

Die Dezentralität der Erzeugung erschwert Cyber-Angriffe

Moderne Gerätefamilien von SMA weisen hoch entwickelte Sicherheitsarchitekturen und komplett andere Zugriffsmechanismen auf, die den in den letzten Jahren stark angestiegenen Sicherheitsanforderungen Rechnung tragen. Aus unserer Sicht erscheint es daher fragwürdig, aus einzelnen Schwachstellen älterer Gerätefamilien auf die Angreifbarkeit aller im Markt befindlichen Solarwechselrichter zu schließen. Es ist nur ein geringer Anteil der SMA-Solar-Inverter mit dem Internet verbunden. Bei den von Herrn Westerhof erwähnten 17 GW sind dies nur etwa 25 Prozent weltweit, also gerade einmal vier GW. Bei einer durchschnittlichen Anlagengröße von vier kW in einem Privathaushalt müssten also in etwa eine Million Router in Privathaushalten gehackt und unter Kontrolle gebracht werden, um eine für das Stromnetz relevante Größenordnung zu erreichen. Die verteilte regenerative Stromerzeugung stellt daher auch in dieser Hinsicht einen Vorteil und keinen Nachteil da. Bedingt durch die Dezentralität der Erzeugung und die Pluralität der Inverterfamilien und -hersteller erfordert ein Angriff einen sehr viel höheren quantitativen Aufwand als bei zentraler Erzeugung. Selbst ein massiver Einsatz von sogenannten Bots würde hier nur eine geringe Wirksamkeit zeigen, da jede Anlage ein individuell konfiguriertes Angriffsprofil benötigen würde.

Wir haben des Weiteren eine detaillierte Analyse der von Willem Westerhof vorgebrachten Schwachstellen durchgeführt und veröffentlicht. Unsere eigene Einschätzung der Kritikalität weicht hier erheblich von der Willem Westerhofs ab. Zwei konkrete Beispiele: So behauptet Willem Westerhof, dass es ihm möglich gewesen wäre, eine manipulierte Firmware erfolgreich auf dem Inverter zu installieren. Dies ist nicht korrekt – die Sunny Explorer Software zeigt ihm zwar die erfolgreiche Übertragung an (was er als „erfolgreiches Flashen" bezeichnet), das neue Binary wird aber faktisch nicht installiert, da es teilweise verschlüsselt ist und weitere Integritätsprüfungen erfolgreich durchlaufen haben muss. Ein Vorgang, der erst nach dem Hochladen durch die geräteinterne Installationsroutine durchgeführt wird.

Darüber hinaus behauptet Willem Westerhof, dass auf den Geräten ein Linux-Betriebssystem laufe und es daher anfällig für Linux-typische Schwachstellen sei. Vor diesem Hintergrund spekuliert er in seiner Darstellung, dass es ein geräteübergreifendes Masterpasswort gäbe, das einen universellen Zugriff erlauben würde. Beides ist falsch. Auf dem von ihm untersuchten Gerät läuft kein Betriebssystem im üblichen Sinne und ein geräteübergreifendes Masterpasswort mit dem man User- oder noch weitergehende Rechte erlangen kann, existiert in keinem unserer Inverter. Weitere Fehler bei der Interpretation der Schwachstellen finden sich in unserer Detailanalyse der CVEs.

Die Befolgung von Richtlinien minimiert das Risiko erfolgreicher Cyber-Attacken

Drei identifizierte Schwachstellen, nämlich die Begrenzung bei der Passwortwahl, die verpflichtende Änderung von initialen Default-Passwörtern sowie ein zusätzlicher Mechanismus zur Verhinderung von Brute-Force-Attacken zum Erraten von Kennwörtern werden im Rahmen eines von uns geplanten Sicherheitsupdates für die betroffenen Produktfamilien derzeit behoben. Diese werden von uns allerdings nicht als so schwerwiegend wie dargestellt eingestuft, wenn die von SMA publizierte Richtlinie zur IT-Sicherheit (http://files.sma.de/dl/7680/CyberSecurity-TI-de-10.pdf) bei Installationen eingehalten wird.

Ein weiteres Szenario – das der Denial-of-Service-Attacken – zeigt in der Realität kaum Auswirkungen. Angriffe durch Denial-of-Service-Attacken sind prinzipiell kaum oder nur mit extrem hohen Aufwand zu verhindern. Diese können aber nur die Datenübertragung der betroffenen Geräte ins Internet stören, im schlimmsten Fall reagiert die Kommunikationsbaugruppe der betroffenen Wechselrichter nicht mehr. Die eigentliche Betriebssoftware der Wechselrichter ist davon nicht betroffen, da sie zum einen unabhängig von der Kommunikations-Baugruppe läuft und zum anderen in vielen Belangen sogar mehrkanalig (redundant) ausgelegt ist. Dies ist schon allein aufgrund der Anforderungen der Netzanschlussrichtlinien sowie der Anforderungen von Berufsgenossenschaft und UL (Underwriter Laboratories, USA) erforderlich. Die Einspeisung bleibt davon unberührt.

Ein Horus-Szenario, also das schlagartige gezielte Abschalten zahlreicher Wechselrichter durch einen Cyber-Angriff, ist extrem unwarscheinlich

Wie schon zuvor ausgeführt: Das Horus-Szenario von Willem Westerhof verallgemeinert Schwachstellen einzelner Geräte auf ein Gesamtportfolio. Die in seiner Analyse dargestellten Schwachstellen reichen nicht aus, um die von ihm dargestellte „Kill-Chain" zu erzeugen, einen schlüssigen Beweis dafür bleibt der Autor sowohl in seinem Vortrag als auch auf seiner Website schuldig. Des Weiteren sind weit weniger Wechselrichter über die Internetschnittstelle zu erreichen – die faktisch vorhandene Pluralität von Geräten, Herstellern und Sicherheitsmechanismen macht einen solchen Angriff daher extrem aufwändig. Die tatsächliche Wahrscheinlichkeit eines erfolgreichen Angriffs schätzen wir vor diesem Hintergrund gering ein, es ist uns bislang auch keinerlei Evidenz bekannt geworden, dass Solarwechselrichter der SMA im realen Betrieb durch Dritte unbefugt beeinflusst wurden.

Fakt ist allerdings, dass mit steigendem Anteil der Solarenergie an der regenerativen Energieerzeugung die Systemrelevanz dieser Energieerzeugungsart steigt. Absolute Sicherheit wird es niemals geben, das zeigen zahlreiche Beispiele anderer sicherheitsrelevanter Branchen. SMA positioniert sich dazu mit einer ständigen Weiterentwicklung der Sicherheitsmaßnahmen. Alle neuen Kommunikationsmechanismen werden ausnahmslos einer Kontrolle externer Sicherheitsfirmen unterzogen, dazu erfolgen regelmäßige Audits unserer Sicherheits-, IT- und Portal-Infrastruktur. Wir arbeiten ständig an neuen Sicherheitskonzepten und haben dazu vielfältige Gremien und Partner. Ein solches „Horus"-Szenario kann niemand komplett ausschließen, aber wir stehen mit unserer Marke dafür ein, dass es so unwahrscheinlich wie möglich wird.

Kommentare zu den CVEs:

Im Folgenden möchten wir die auf der Webseite https://horusscenario.com/CVE-Information/ zitierten Schwachstellen im Einzelnen wie folgt kommentieren. Die CVE (Common Vulnerabilities and Exposures) Texte werden aus Gründen der Übersichtlichkeit hier nur auszugsweise dargestellt. Die Einschätzung der Kritikalität (CVSS-Vektoren) haben wir durch unsere eigene Einschätzung in Bezug auf eine Massenmanipulation der Inverter ergänzt (auf der üblichen Skala 0 bis 10 von unkritisch bis kritisch).

Wir weisen nochmals darauf hin, dass die in den CVE-Texten regelmäßig benutzte Einleitung *„An issue was discovered in SMA Solar Technology products"* sich jeweils nur auf wenige, ältere Gerätebaureihen bezieht. Die Geräte der aktuellen Entwicklungsgeneration weisen ein komplett anderes Betriebssystem sowie eine sicherheitstechnisch erheblich weiterentwickelte Konfigurations- und Steuerungsumgebung auf.

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.

Selbst wenn dies ausgenutzt wird, entsteht außer einem Kommunikationsausfall kein weiterer Schaden. Der Wechselrichter arbeitet wie bisher weiter, lediglich das (nicht auf dem Wechselrichter laufende und zur Inbetriebnahme oder zum Service genutzte Programm) Sunny Explorer muss neu gestartet werden. Eine Telnet-Attacke hinter der Firewall des Heimnetzwerks ist nur möglich, wenn vorher die Firewall des Routers manipuliert wurde oder Sicherheitsregeln des Routers ausser Kraft gesetzt wurden. Außerhalb des lokalen Netzwerks ist eine Kommunikation zwischen der Applikation Sunny Explorer und dem Wechselrichter nicht möglich.

[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)

Rating suggested by SMA:
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.

Es liegt in der Verantwortung des Anlagenbetreibers / Installateurs, Passworte zu vergeben die ein Mindestmaß an Komplexität aufweisen. Als Hersteller weisen wir sowohl in Dokumentation als auch in unseren Sicherheitsrichtlinien deutlich darauf hin. Auf die Vergabe der Passwörter haben wir keinen Einfluss, ebenso wenig wollen und können wir die Passwörter kontrollieren.

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.

In der Tat ist dies eine auch von uns beobachtete Praxis bei Installateuren und Anlagenüberwachern (aus Bequemlichkeit). In unseren Sicherheitsleitfaden wird explizit darauf hingewiesen, dieser Praxis nicht mehr zu folgen.

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.

Der Autor scheint die GridGuard-Code Funktionalität gründlich missverstanden zu haben. GridGuard-Code ist per se KEIN Security-Feature, hierbei geht es nur darum, Veränderungen an netzrelevanten Parametern namentlich rückverfolgbar zu machen. Daher ist der hierfür vergebene Code an eine Person, nicht an den Inverter gebunden und bei SMA die Identität der an den Code gebundenen Person registriert. Es handelt sich daher um eine Art elektronische Identität, deren Aktivität z.B. im Log des Inverters vermerkt wird. Der GridGuard-Code ist jeweils nur in Verbindung mit dem (individuell gesetzten) Installateurs-Passwort des Gerätes nutzbar, er kann nicht alleinig zum Login in das Gerät genutzt werden.

Im Übrigen wird der GridGuard-Code üblicherweise nur für die Inbetriebnahme verwendet, dann auch nur in Ausnahmefällen. Es gibt in der Tat neben den Installateur- und Betreiber-Accounts noch Service- und Entwickler-Accounts, die z.B. für Reparatur- und Servicezwecke genutzt werden (damit muss ein Benutzer oder Installateur sein persönliches Passwort nicht kompromittieren, wenn er ein Gerät zur Reparatur einschickt oder der SMA Service vor Ort am Gerät tätig wird). Diese Accounts dienen rein einer tiefergehenden Diagnose des Geräts und haben ebenfalls geräteindividuelle sichere Passwörter. Sie werden ausschließlich durch SMA Personal genutzt und auch nur, wenn der Anlagenbetreiber / -eigner dies dem SMA Service ausdrücklich gestattet.

Globale, hart-kodierte Masterpasswörter existieren entgegen der Behauptungen von Herrn Westerhof NICHT.

[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)

Rating suggested by SMA:
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.

Diese Komplexität war zum Zeitpunkt der Entwicklung der betroffenen Wechselrichter Stand der Technik. Ein 12 Zeichen langes, case-sensitives Passwort bestehend aus Buchstaben, Ziffern und gängigen Sonderzeichen bietet bereits eine recht hohe Sicherheit. Exotische Sonderzeichen werden unserer Erfahrung nach in der Praxis zudem höchst selten genutzt.

Nichtsdestotrotz wird SMA wird in Kürze ein Firmware-Update für die Geräte bereitstellen, das beliebige Passwörter erlaubt, die Änderung von initialen Default-Passwörtern erzwingt sowie einen Schutz gegen Brute-Force Passwortattacken bietet.

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

Siehe Erläuterung zu 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)

Rating suggested by SMA: 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.

Damit ist ein „Mitschneiden" einer internen Sunny Explorer Session gemeint. Das bedingt natürlich, dass dieses Tool (welches ein reines Inbetriebnahme- und Servicetool ist), genau in dem Moment des Mitschneidens die vom Hacker gewünschte Aktion vornimmt. Die tatsächliche Wahrscheinlichkeit dafür ist gering, da es üblicherweise nur einmalig während der Installation aktiviert wird.

[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.

Siehe Erläuterung zu CVE-9852 (Doublette).

[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)

Rating suggested by SMA: 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.

Auch für diesen CVE ist ein bereits gehacktes, lokales Netzwerk Grundvoraussetzung. Darüber hinaus findet eine solche Authentisierung bei der Inbetriebnahme mittels Sunny Explorer üblicherweise nur einmalig statt.

[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)

Rating suggested by SMA: 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.

Dies ist genereller Stand der Technik innerhalb abgeschotteter Teilnetzwerke, auch im Energiesektor oder im Smart Home Bereich. In diesem Umfeld werden ansonsten Protokolle wie Modbus/TCP, IEC60870 und IEC61850 verwendet, welche ebenfalls ohne Verschlüsselung übertragen werden. Es handelt sich daher dabei nicht um eine SMA-spezifische Verletzlichkeit. Um eine grundsätzliche Sicherheit in dieser Hinsicht herzustellen, weisen wir auf die Beachtung unserer Guideline hin (http://files.sma.de/dl/7680/CyberSecurity-TI-de-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)

Rating suggested by SMA:
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.

Siehe CVE-2017-9852. Das Vorhandensein zusätzlicher Accounts ist keine Sicherheitslücke per se, solange diese mit geräteindividuellen, sicheren Passwörtern geschützt sind. Diagnosezugänge sind bei allen softwarekonfigurierbaren, technischen Anlagen Stand der Technik und nicht per default unsicher.

[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)

Rating suggested by SMA:
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.

Theoretisch wäre ein cracken des REGISTER Requests möglich. Aber: Zusätzlich muss man aber eine Kombination von PIC (Product Identification Code) und RID (Registration Identification) bereithalten, die sich von bereits vergebenen PIC und RID unterscheidet und zudem vom SMA Registrierungsserver als gültig eingestuft wird. Die nach einer erfolgreichen Registrierung erlaubte Nutzdatenkommunikation verwendet kein SIP-Protokoll und ist zudem nach SHA-256 – also gemäß aktuellem Stand der Technik – verschlüsselt. In der Praxis stufen wir die Erfolgswahrscheinlichkeit für eine solche Manipulation als höchst gering ein.

[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)

Rating suggested by SMA:
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.

Dies ist eine Behauptung, die schlichtweg nicht stimmt. Die für ein Firmware-Update notwendigen Maßnahmen sind Herrn Westerhof augenscheinlich nicht bekannt, er hat auch keinen Beweis dafür, dass er das erwähnte Update erfolgreich durchgeführt hat. Sunny Explorer mag den Anschein erweckt haben, dass die geschilderte Aktion erfolgreich war, in der Tat wird dort nur vermeldet, dass

die Datei komplett übertragen wurde. Eine letztendliche Prüfung auf Integrität und Kompatibilität findet erst nach der Übertragung mittels eines komplexen Verfahrens durch die Installationsroutine auf dem Inverter statt.

[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)

Rating suggested by SMA:
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.

Siehe Erläuterung zu 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)

Rating suggested by SMA: 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.

Die ist prinzipiell möglich, aber die in dem Debug-Report enthaltenen Informationen sind von marginaler Bedeutung für einen Hacker, sie enthalten z.B. keinerlei User- und Passwortinformationen. Dies wird von beiden Seiten als unkritisch eingestuft.

[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)

Rating suggested by SMA: 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.

Dies ist in der Praxis höchst unwahrscheinlich, weil es nur zum Tragen kommen kann, wenn zeitgleich der Sunny Explorer zum Service/ Inbetriebnahme genutzt wird UND zugleich ein Host mit Schadsoftware kontaktiert wird UND dieser Host auch noch spezifisch für eine Manipulation der Parameter dieser speziellen Geräte eingerichtet ist.

[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)

Rating suggested by SMA: 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.

Der Zeitstempel wird in den Geräten lediglich für die zeitliche Kennzeichnung der Logeinträge genutzt, der Nutzen, den ein Hacker daraus ziehen kann ist absolut marginal. Es gibt in den Geräten weder Lockout-Policies noch Zufallsgeneratoren, die auf dem Zeitstempel basieren, dies ist pure Spekulation seitens Herrn Westerhof. Außerdem wird bei einer Online-Verbindung die Systemzeit kurze Zeit später (spätestens, wenn sich ein zugelassener User einloggt) wieder mit einer gültigen NTP-Zeit synchronisiert.

[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)

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

Zusammenfassende Bewertung:

Von den 14 genannten Vulnerabilities stuft Herr Westerhof zwei (9853 und 9862) selbst als völlig unkritisch ein. Bei zwei weiteren kommt Herr Westerhof aufgrund ungenügendem Verständnis oder wilder Spekulationen zu einer deutlich zu hohen Kritikalität (z.B. bei seiner Annahme in 9864, dass eine unauthorisierte Änderung des Timestamps Folgewirkungen haben könnte, 9855). Drei weitere beschreiben Szenarien, die extrem unwahrscheinlich sind oder auf Ereignissen beruhen, die nur einmalig beim Einrichten der Anlage vorkommen und daher für die Zugriffsgewinnung für einen Massenangriff völlig ungeeignet sind (9863, 9859, 9854), zwei weitere beruhen auf falschen Erkenntnissen (9860: erfolgreicher Firmware-Update ohne Authentifizierung möglich; 9861: Das SIP Protokoll wird nicht zur Datenübertragung benutzt, nur zum Verbindungsaufbau). Zwei weitere beschreiben einen absolut üblichen Stand der Technik (9857, 9858). Auch ein „crashen" eines Inbetriebnahmeprogramms ohne weitere Folgen (9851) ist kaum ein Argument für eine „Kill Chain". Aus unserer Sicht verbleiben im Wesentlichen die aus heutiger Perspektive nicht mehr ganz zeitgemäße Passwortarchitektur (Fehlender Zwang zur Default-Passwortänderung und Einschränkungen bei Passwort-Zeichen und –Länge) sowie eine fehlende Sperre für Brute-Force Angriffe auf das Passwort. Beides führt aber bei sachgemäßer Installation innerhalb eines geschlossenen Netzwerks nach unserer Cybersicherheitsrichtlinien und dem Setzen eines adäquaten Passworts zu einem sicheren System. Nichtsdestotrotz werden wir hierzu für die vier Gerätefamilien zeitnah ein Firmware-Update zur Adressierung dieser Thematik zur Verfügung stellen.

Bitte sprechen Sie uns an, wenn Sie weitere Fragen zur Sicherheit unserer Produkte haben. Wir stehen Ihnen jederzeit zur Verfügung.