# Schneider Electric Sicherheitshinweis

## Easergy T300

**09. Juni 2020**

## Einleitung

Forscher der Rostelecom-Solar haben Schneider Electric auf mehrere Schwachstellen im Produkt Easergy T300 aufmerksam gemacht. Schneider Electric hat bei der Behebung dieser Schwachstellen eng mit diesen Forschern kooperiert. Für die gute Zusammenarbeit und Transparenz bedanken wir uns. Die Schwachstellen wurden mittels eines kostenfreien Firmware-Updates behoben, das ab sofort auf Anfrage beim Schneider Electric Customer Care Center erhältlich ist.

Für die Ausnutzung der meisten gemeldeten Schnittstellen ist ein Zugriff auf das Kundennetzwerk erforderlich. Das Risiko einer Ausnutzung kann also wesentlich minimiert werden, wenn das Kundennetzwerk gut geschützt ist und auf externe Angriffe überwacht wird sowie nur Software-Updates von vertrauenswürdigen Quellen eingespielt werden.

Schneider Electric empfiehlt seinen Kunden, das Produkt so bald als möglich mit der neuen Firmware upzudaten. Außerdem sollte darauf geachtet werden, dass Firmwaredateien, mit denen das Produkt upgedatet wird, nur aus vertrauenswürdigen Quellen stammen, dass das Produkt in ordnungsgemäß segmentierten Steuernetzwerken betrieben wird, dass jeder Arbeitsplatz, der für den Zugriff auf das Produkt konfiguriert ist, entsprechend gesichert wurde, und dass die unten beschriebenen Abhilfe- und allgemeinen Sicherheitsempfehlungen befolgt werden.

## Betroffene Produkte

Easergy T300 mit Firmware 1.5.2 und älter

Easergy T300 ist eine modulare Plattform für die Netzautomatisierung, die typischerweise in Mittelspannungsschaltanlagen (2400 bis 69000 V AC) zum Einsatz kommt.

## Details

CVE ID: **CVE-2020-7503**

CVSS v3.0 Base Score 8.8 | High | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Es liegt eine Schwachstelle der Kategorie CWE-352 (Cross-Site Request Forgery, CSRF) vor, die einen Angreifer in die Lage versetzen könnte, XSRF-Tokendaten abzufangen und schädliche Befehle im Namen eines autorisierten Nutzers auszuführen.

# Schneider Electric Sicherheitshinweis

CVE ID: **CVE-2020-7504**

CVSS v3.0 Base Score 5.3 | Medium | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

Es liegt eine Schwachstelle der Kategorie CWE-20 (Improper Input Validation) vor, die einen Angreifer in die Lage versetzen könnte, bestimmte Netzwerkpakete zu senden und den Webserver-Dienst im Produkt zu deaktivieren.

CVE ID: **CVE-2020-7505**

CVSS v3.0 Base Score 6.1 | Medium | CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:H/A:H

Es liegt eine Schwachstelle der Kategorie CWE-494 (Download of Code Without Integrity Check) vor, die einen Angreifer in die Lage versetzen könnte, Daten mit gefährlichem Inhalt in die Firmware einzuspielen und beliebige Codes auf dem Zielsystem auszuführen.

CVE ID: **CVE-2020-7506**

CVSS v3.0 Base Score 7.5 | High | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Es liegt eine Schwachstelle der Kategorie CWE-538 (File and Directory Information Exposure) vor, die einen Angreifer in die Lage versetzen könnte, das Archive mit der Firmware für den Controller und die Module mit dem üblichen TAR-Archivierungsprogramm zu packen bzw. zu entpacken, was zu einer Offenlegung von Informationen führt.

CVE ID: **CVE-2020-7507**

CVSS v3.0 Base Score 9.3 | Critical | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:H

Es liegt eine Schwachstelle der Kategorie CWE-400 (Uncontrolled Resource Consumption) vor, die einen Angreifer in die Lage versetzen könnte, durch vielfach wiederholte Anmeldeversuche einen Denial-of-Service zu verursachen.

CVE ID: **CVE-2020-7508**

CVSS v3.0 Base Score 9.8 | Critical | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Es liegt eine Schwachstelle der Kategorie CWE-307 (Improper Restriction of Excessive Authentication Attempts) vor, die einen Angreifer in die Lage versetzen könnte, durch Brute-Force-Methoden vollen Zugriff zu erlangen.

CVE ID: **CVE-2020-7509**

CVSS v3.0 Base Score 9.0 | Critical | CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:H/A:H

Es liegt eine Schwachstelle der Kategorie CWE-269 (Improper Privilege Management) vor, die einen Angreifer in die Lage versetzen könnte, sich mehr Berechtigungen zu verschaffen und Dateien zu löschen.

# Schneider Electric Sicherheitshinweis

CVE ID: **CVE-2020-7510**

CVSS v3.0 Base Score 8.6 | High | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

Es liegt eine Schwachstelle der Kategorie CWE-200 (Information Exposure) vor, die einen Angreifer in die Lage versetzen könnte, Systeminformationen auszulesen.

CVE ID: **CVE-2020-7511**

CVSS v3.0 Base Score 8.6 | High | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

Es liegt eine Schwachstelle der Kategorie CWE-327 (Use of a Broken or Risky Cryptographic Algorithm) vor, die einen Angreifer in die Lage versetzen könnte, durch Brute-Force-Methoden ein Passwort zu erlangen.

CVE ID: **CVE-2020-7512**

CVSS v3.0 Base Score 5.3 | Medium | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Es liegt eine Schwachstelle der Kategorie CWE-1103 (Use of Platform-Dependent Third Party Components) vor, die einen Angreifer in die Lage versetzen könnte, eine Drittkomponente mit Schwachstellen auszunutzen.

CVE ID: **CVE-2020-7513**

CVSS v3.0 Base Score 7.4 | High | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N

Es liegt eine Schwachstelle der Kategorie CWE-312 (Cleartext Storage of Sensitive Information) vor, die einen Angreifer in die Lage versetzen könnte, Datenverkehr abzufangen und Konfigurationsdaten auszulesen.

## Abhilfemaßnahmen

Diese Schwachstellen wurden in der T300-Firmwareversion 2.7 behoben. Die Firmware ist erhältlich beim Schneider Electric Customer Care Center.

Zur Risikominimierung werden ferner die folgenden Maßnahmen empfohlen:

- Die Firmware muss aus einer vertrauenswürdigen Quelle stammen und ihre Datenintegrität geschützt sein.
- Ein separates, sicheres lokales Netzwerk und eine sichere Zugriffssteuerung müssen verwendet werden.

# Schneider Electric Sicherheitshinweis

## Produktinformationen

Das Fernwirkgerät Easergy T300 ist eine modulare Hardware- und Firmware-Plattform für Anwendungen in Verteilnetzen. Sie kommt typischerweise in Mittelspannungsschaltanlagen (2400 bis 69000 V AC) zum Einsatz.

**Produktkategorie -** Mittelspannungsverteilung und Netzautomatisierung

Erfahren Sie mehr über die Produkte von Schneider Electric: www.se.com/de/de/all-products

## Allgemeine Sicherheitsempfehlungen

Wir empfehlen dringend, die folgenden branchenspezifischen Best Practices zur Cybersicherheit anzuwenden:

- Stellen Sie sicher, dass Steuerungs- und Sicherheitsnetzwerke sowie Remote-Geräte durch Firewalls geschützt sind und isolieren Sie sie vom Betriebsnetzwerk.
- Richten Sie physische Kontrollen ein, so dass Unbefugten der Zugriff auf ICS-Systeme, Komponenten, Peripheriegeräte und Netzwerke verwehrt wird.
- Alle Controller sollten in verschlossenen Schränken installiert und nie im Programmiermodus belassen werden.
- Verbinden Sie niemals Programmiersoftware mit anderen Netzwerken als dem, für dessen Geräte sie bestimmt ist.
- Scannen Sie alle Datenträger, die zum Datenaustausch mit dem isolierten Netzwerk verwendet werden, wie CDs, USB-Sticks etc., vor ihrem Einsatz an den Terminals oder jedem Knoten, der an diese Netzwerke angeschlossen ist.
- Verbinden Sie niemals ohne entsprechende Cybersicherheitsmaßnahmen Laptops, die außer an das vorgesehene Netzwerk noch an andere Netzwerke angeschlossen waren, mit dem Sicherheits- oder Steuerungsnetzwerk.
- Minimieren Sie die Netzwerk-Exposition von Steuerungs- oder Leitsystemen bzw. Geräten der Steuerungs- oder Leitsysteme und stellen Sie sicher, dass nicht über das Internet auf sie zugegriffen werden kann.
- Wenn ein Remote-Zugriff erforderlich ist, nutzen Sie sichere Verfahren, z. B. Virtual Private Networks (VPNs). Beachten Sie aber, dass auch VPNs Schwachstellen haben können und deshalb regelmäßiger Updates bedürfen, und dass VPNs stets nur so sicher sind, wie die daran angeschlossenen Geräte.

# Schneider Electric Sicherheitshinweis

## Danksagungen

Schneider Electric dankt den folgenden Personen für die Unterstützung bei der Identifizierung dieser Schwachstelle sowie bei der Koordinierung der Abhilfemaßnahmen:

| CVE | Name |
|---|---|
| CVE-2020-7503, CVE-2020-7504, CVE-2020-7505, CVE-2020-7506, CVE-2020-7507, CVE-2020-7508, CVE-2020-7509, CVE-2020-7510, CVE-2020, 7511, CVE-2020-7512, CVE-2020-7513 | Evgeniy Druzhinin und Ilya Karpov (Rostelecom-Solar) |

## Weiterführende Informationen

Dieses Dokument beschreibt die identifizierte(n) Schwachstelle(n) und die zu ihrer Behebung erforderlichen Maßnahmen. Für weitere Informationen und Support zum Schutz Ihrer Anlage, kontaktieren Sie Ihren Schneider Electric Ansprechpartner bzw. den Schneider Electric Cyber Security Support. Diese sind über die Angelegenheit informiert und können Sie während des gesamten Prozesses unterstützen.

https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

https://www.se.com/ww/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

# Schneider Electric Sicherheitshinweis

## Über Schneider Electric

Wir bei Schneider Electric glauben, dass der **Zugang zu Energie und digitaler Technologie** ein grundlegendes Menschenrecht ist. Unser Ziel ist es, **dass verfügbare Energie und Ressourcen bestmöglich genutzt werden**, nach dem Motto „**Life is On**“ – überall, für jeden, jederzeit.

Wir bieten **digitale Energie- und Automatisierungslösungen** für **Effizienz und Nachhaltigkeit**. Wir kombinieren weltweit führende Energietechnologien, Automatisierung in Echtzeit, Software und Services zu integrierten Lösungen für Haushalte, Gebäude, Rechenzentren, Infrastrukturen und Industrie.

Wir streben danach, das volle Potential einer **offenen, globalen und innovativen Gemeinschaft** auszuschöpfen, die sich mit der **Sinnhaftigkeit unserer Ziele** und unseren Werten der **Inklusion und Förderung** identifiziert.

www.se.com

Versionsübersicht:

| | |
|---|---|
| **Version 1**<br>*9. Juni 2020* | Originalausgabe |