

Schneider Electric Sicherheitshinweis

Easergy Builder

09. Juni 2020

Einleitung

Forscher der Rostelecom-Solar haben Schneider Electric auf mehrere Schwachstellen im Konfigurationswerkzeug Easergy Builder aufmerksam gemacht. Schneider Electric hat bei der Behebung dieser Schwachstellen eng mit Ilya Karpov and Evgeniy Druzhinin von Rostelecom-Solar kooperiert und dankt für die gute Zusammenarbeit und Transparenz. Die Schwachstellen wurden mittels eines kostenfreien Software-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 Software 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 Builder Version 1.4.7.2 und älter

Easergy Builder wird von den Engineering-Teams zur Konfiguration der Easergy T300 Netzautomatisierungs-Plattform genutzt.

Details

CVE ID: **CVE-2020-7514**

CVSS v3.0 Base Score 8.4 | High | CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Es liegt eine Schwachstelle der Kategorie CWE-327 (Use of a Broken or Risky Cryptographic Algorithm) vor, die einem Angreifer Zugang zu den Autorisierungskennndaten und damit vollen Zugriff auf das Gerät ermöglichen könnte.

Schneider Electric Sicherheitshinweis

CVE ID: **CVE-2020-7515**

CVSS v3.0 Base Score 8.4 | High | CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Es liegt eine Schwachstelle der Kategorie CWE-321 (Use of Hard-Coded Cryptographic Key Stored in Cleartext) vor, die einen Angreifer in die Lage versetzen könnte, ein Passwort zu entschlüsseln.

CVE ID: **CVE-2020-7516**

CVSS v3.0 Base Score 8.4 | High | CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Es liegt eine Schwachstelle der Kategorie CWE-316 (Cleartext Storage of Sensitive Information in Memory) vor, die einem Angreifer den Zugang zu Anmeldekenndaten ermöglichen könnte.

CVE ID: **CVE-2020-7517**

CVSS v3.0 Base Score 7.1 | High | CVSS:3.0/AV:L/AC:L/PR:N/UI:N/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, Benutzerkenndaten auszulesen.

CVE ID: **CVE-2020-7518**

CVSS v3.0 Base Score 8.2 | High | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:H

Es liegt eine Schwachstelle der Kategorie CWE-20 (Improper Input Validation) vor, die einen Angreifer in die Lage versetzen könnte, Projektkonfigurationsdateien zu ändern.

CVE ID: **CVE-2020-7519**

CVSS v3.0 Base Score 7.3 | High | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Es liegt eine Schwachstelle der Kategorie CWE-521 (Weak Password Requirements) vor, die einen Angreifer in die Lage versetzen könnte, Benutzerkonten zu ändern.

Abhilfemaßnahmen

Diese Schwachstellen wurden in der Easergy Builder Version 1.6.3.0 behoben. Die Software ist erhältlich beim [Schneider Electric Customer Care Center](#).

Schneider Electric Sicherheitshinweis

Zur Risikominimierung werden ferner die folgenden Maßnahmen empfohlen:

- Ein separates, sicheres lokales Netzwerk und eine sichere Zugriffssteuerung müssen verwendet werden.

Produktinformationen

Easergy Builder wird von den Engineering-Teams zur Konfiguration der Easergy T300 Netzautomatisierungs-Plattform genutzt.

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-2020-7514, CVE-2020-7515, CVE-2020-7516, CVE-2020-7517, CVE-2020-7518, CVE-2020-7519	Ilya Karpov und Evgeniy Druzhinin (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>

Rechtliche Hinweise

DIESES DOKUMENT SOLL EINEN ÜBERBLICK ÜBER DIE IDENTIFIZIERTE SCHWACHSTELLE UND DIE VORGESCHLAGENEN ABHILFEMASSNAHMEN, SANIERUNGS-, BEHELFS- UND/ODER ALLGEMEINEN SICHERHEITSEMPFEHLUNGEN GEBEN UND WIRD IN DER VORLIEGENDEN FORM UND OHNE JEGLICHE GEWÄHRLEISTUNG BEREITGESTELLT. SCHNEIDER ELECTRIC SCHLIESST ALLE GEWÄHRLEISTUNGEN AUS, GLEICH OB AUSDRÜCKLICH ODER KONKLUDENT, EINSCHLIESSLICH GEWÄHRLEISTUNGEN DER HANDELSÜBLICHKEIT ODER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK. SCHNEIDER ELECTRIC HAFTET IN KEINEM FALL FÜR SCHÄDEN JEGLICHER ART, EINSCHLIESSLICH DIREKTER, INDIREKTER, ZUFÄLLIGER SCHÄDEN, FOLGESCHÄDEN, ENTGANGENER GESCHÄFTSGEWINNE ODER BESONDERER SCHÄDEN, SELBST WENN SCHNEIDER ELECTRIC ÜBER DIE MÖGLICHKEIT SOLCHER SCHÄDEN INFORMIERT WURDE. DIE NUTZUNG DIESES SICHERHEITSHINWEISES, DER DARIN ENTHALTENEN INFORMATIONEN ODER DER DAMIT VERBUNDENEN MATERIALIEN ERFOLGT AUF EIGENE GEFAHR. SCHNEIDER ELECTRIC BEHÄLT SICH DAS RECHT VOR, DIESEN SICHERHEITSHINWEIS JEDERZEIT UND NACH EIGENEM ERMESSEN ZU AKTUALISIEREN ODER ZU ÄNDERN.

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 <i>9. Juni 2020</i>	Originalausgabe
---	------------------------