



SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Framework für Angriffe auf ICS- und SCADA-Systeme (INCONTROLLER / PIPEDREAM)

CSW-Nr. 2022-215481-1032, Version 1.0, 14.04.2022

IT-Bedrohungslage*: 2 / Gelb

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:WHITE: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Sachverhalt

Am 13.4.2022 wurde durch die US-Behörden CISA, DOE, NSA und FBI ein gemeinsames Security Advisory veröffentlicht, welches verschiedene Tools beschreibt, die zum Einsatz gegen industrielle Steuerungs- und Automatisierungssysteme entwickelt wurden [CIS2022]. Die Firma Dragos verwendet den Namen "PIPEDREAM" [DRA2022]. Mandiant bezeichnet in seinem Bericht das Toolkit als "INCONTROLLER" [MAN2022].

Das Framework besteht aus den folgenden Komponenten, die gemeinsam oder unabhängig voneinander eingesetzt werden können:

- * 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
 2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
 3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
 4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

Dragos Name	Mandiant Name	Beschreibung
EVILSCHOLAR	CODECALL	Tool für die Erkennung, Zugriff, Manipulation und Abschaltung von Schneider Electric PLCs. Es enthält Modbus und CODESYS Funktionalitäten
BADOMEN	OMSHELL	Tool zum Auffinden, Identifizieren und Interagieren mit OMRON PLCs
MOUSEHOLE	TAGRUN	Tool zur Interaktion (Verbinden, Lesen und Schreiben) mit OPC-UA Servern
DUSTTUNNEL	ICECORE	Tool für Reconnaissance und Command and Control
LAZYCARGO		Tool zum Ausnutzen von CVE-2020-15368 im AsrDrv103.sys (Treiber für ASRock Motherboards)

Die ICS-spezifischen Tools sind modular aufgebaut. Es werden **keine spezifischen Schwachstellen ausgenutzt**. Vielmehr werden legitime Funktionen verwendet, um die gewünschten Ziele zu erreichen. Somit ist die Funktionalität mit einer legitimen Programmierstation vergleichbar. Nach bisherigen Erkenntnissen wurden die Tools entdeckt, bevor sie eingesetzt werden konnten.

Es ist nicht bekannt, welche Tools die Angreifer für die initiale Infektion nutzen würden. Einige mögliche Szenarien werden in dem Bericht beschrieben.

Die Tools des Frameworks setzen unter anderem auch Brute-Force-Angriffe mit Wörterbüchern gegen Systeme ein, die mit Passwörtern abgesichert sind.

Weitere Details können den Berichten [CIS2022], [MAN2022] und [DRA2022] entnommen werden.

Bewertung

Ein Angriff und Einsatz der ICS-spezifischen Tools des Frameworks erscheint vor allem im Prozessnetz zielführend.

Das BSI geht, aufgrund der hohen Verbreitung der bedrohten Systeme in verschiedene Branchen, von einer hohen Relevanz aus. Wenngleich ein aktiver Einsatz des Frameworks bislang nicht bekannt ist, erhöht die Existenz das Bedrohungsszenario für ICS-Systeme.

Der modulare Aufbau der einzelnen Tools legt nahe, dass die Angreifergruppe diese Tools über einen längeren Zeitraum einsetzen möchte. Durch die Modularität sinkt der Aufwand, die Tools für andere Geräte nutzbar zu machen. Durch die Implementierung des weit verbreiteten Protokolls Modbus und von CODESYS kann nicht ausgeschlossen werden, dass andere Geräte, welche eine dieser Technologien einsetzen, ebenfalls angreifbar sind.

Detektionsmethoden, die auf IoCs beruhen, werden als problematisch bewertet, da sich die Indikatoren durch mit an Sicherheit grenzender Wahrscheinlichkeit vorgenommenen Anpassungen an die Infrastruktur der Opfer unterscheiden würden.

Maßnahmen

Die konsequente Trennung von Büro- und Prozessnetz und die Überwachung von Schnittstellen zwischen den Netzen ist eine der wichtigsten Maßnahmen. Kommunikation des Prozessnetzes mit anderen Netzen sollten auf das Minimum beschränkt werden. Es muss sichergestellt werden, dass alle Schnittstellen bekannt sind. Jegliche Zugriffe auf das Prozessnetz aus anderen Netzen müssen angemessen abgesichert sein. Dies gilt sowohl für Zugriffe aus dem Büronetz und Fernwartungszugriffe als auch Herstellerzugänge. Insbesondere müssen auch Mobilfunkmodems im Prozessnetz

entsprechend geschützt und überwacht werden. Wo immer möglich, sollte Multifaktorauthentisierung eingesetzt werden. Sofern Daten aus dem Prozessnetz direkt ins Internet übertragen werden, muss dies rückwirkungsfrei geschehen.

Eine starke Segmentierung mit wirksamen Begrenzungen der Kommunikation der Segmente untereinander auf das absolute Minimum, kann die Ausbreitung der Angreifer im Netz erschweren. Insbesondere sollten die Kommunikationspartner, welche kritische Befehle (Schreiboperationen, Zustandsänderungen, Firmware-Updates,...) ausführen dürfen, explizit gewhitelistet sein und diese Kommunikation überwacht werden.

Für nicht Standard-IT-Geräte, die einen Passwortschutz bereitstellen (Purdue-Level 2 und 3), sollten die Passwörter gesetzt werden beziehungsweise Default-Zugangsdaten geändert werden. Sofern diese Geräte keine ausreichend komplexen Passwörter unterstützen, sollten die Passwörter in regelmäßigen Abständen geändert werden.

Statt einem auf Indikatoren basierenden Detektionsansatz, sollte ein verhaltensbasierter Ansatz gewählt werden. Dazu zählt insbesondere die Anomaliedetektion. Hierfür müssen ausreichend Daten durch Logging und Netzwerk-Monitoring erhoben werden. Darüber hinaus sollten regelmäßig Threat Huntings durchgeführt werden.

Für einen Exploit der ASRock-Treiber-Schwachstelle, stellt Mandiant Yara-Regeln bereit. Diese sind der Meldung beigelegt.

Ein Notfallplan, der die relevanten Parteien aus IT, Cybersicherheit und Betrieb einbindet, muss existieren, bekannt sein und beübt werden. Symptome, wie beispielsweise DoS und Verbindungsabbrüche, müssen untersucht werden, da dies auf Angreiferaktivität hindeuten kann.

Gerätespezifische Hinweise gibt Schneider Electric in seinem Security Bulletin [SCE2022].

Des Weiteren kann die Angriffsfläche durch eine konsequente Anwendung der Defense-in-Depth-Strategie minimiert werden. Hinweise hierzu finden sich auch im ICS-Kompodium des BSI [BSI2013].

Links

[BSI2013] ICS-Security-Kompodium

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompodium_pdf.html

[CIS2022] Alert (AA22-103A): APT Cyber Tools Targeting ICS/SCADA Devices

<https://www.cisa.gov/uscert/ncas/alerts/aa22-103a>

[DRA2022] PIPEDREAM: CHERNOVITE'S EMERGING MALWARE TARGETING INDUSTRIAL CONTROL SYSTEMS

https://hub.dragos.com/hubfs/116-Whitepapers/Dragos_ChernoviteWP_v2b.pdf

[MAN2022] INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems

<https://www.mandiant.com/resources/incontroller-state-sponsored-ics-tool>

[SCE2022] Schneider Electric Security Bulletin SESB-2022-01

https://download.schneider-electric.com/files?p_Doc_Ref=SESB-2022-01

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs) welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

- 1) Was ist das Traffic Light Protokoll?
Das TLP ist ein von der OECD entworfenes Protokoll, welches die Weitergabe von sensiblen Informationen innerhalb eines Informationsverbundes regelt. Die vom Autor adressierten Empfänger dieses Dokumentes haben sich im Vorfeld schriftlich verpflichtet das TLP zu beachten und das Dokument entsprechend den „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten.
- 2) Welche Einstufungen existieren?
 - **TLP:WHITE: Unbegrenzte Weitergabe**
Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.
 - **TLP:GREEN: Organisationsübergreifende Weitergabe**
Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.
 - **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Verteilung**
Informationen dieser Stufe darf der Empfänger innerhalb seiner Organisation auf Basis „Kenntnis nur wenn nötig“ weitergeben. Der Empfänger darf die Informationen zudem an Dritte weitergeben, soweit diese die Informationen zum Schutz des Empfängers oder zur Schadensreduktion beim Empfänger benötigen. Hierfür muss er sicherstellen, dass die „Dritten“ das TLP kennen und die damit verbundenen Regeln einhalten. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
 - **TLP:RED: Persönlich, nur für benannte Empfänger**
Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. Meistens werden TLP:RED-Informationen mündlich oder persönlich übergeben.
- 3) Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?
Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.
- 4) Was passiert, wenn ich die Einstufung nicht beachte?
Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:WHITE eingestufte Informationen aus dem Kreis der Verpflichteten.