SANS

How can organizations prepare their IT and OT teams to be ready for security incidents?

Don C. Weber / Cutaway Security, LLC

SANS ICS410: ICS/SCADA Security Essentials

Assessing and Exploiting Control Systems

- ICS Security Program Maturity Analysis
- ICS Security Assessments
- Penetration Testing
- Security Research

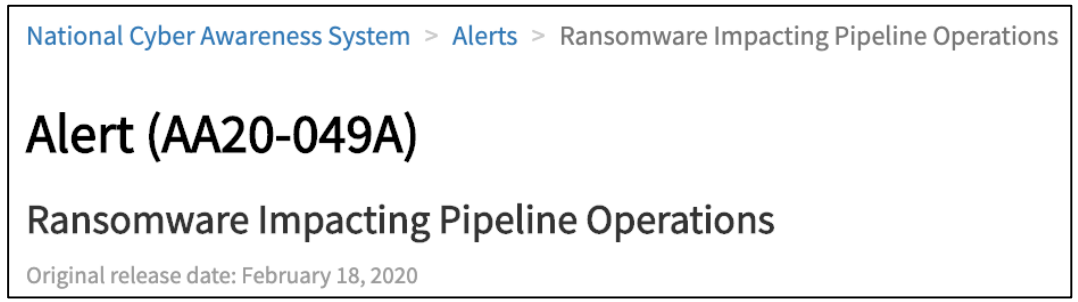
CUTAWAY SECURITY
INFOSEC CONSULTANTS

Who's the Operator / Hacker / Criminal?

Image Source: https://www.controlthings.io/ - Accessing and Exploiting Control Systems

https://foursquare.com/v/dcs-control-room-pt-indolampung-distillery/4fc84b41e4b005dcbe5f17d0/photos

Targeted Attacks on Control Networks

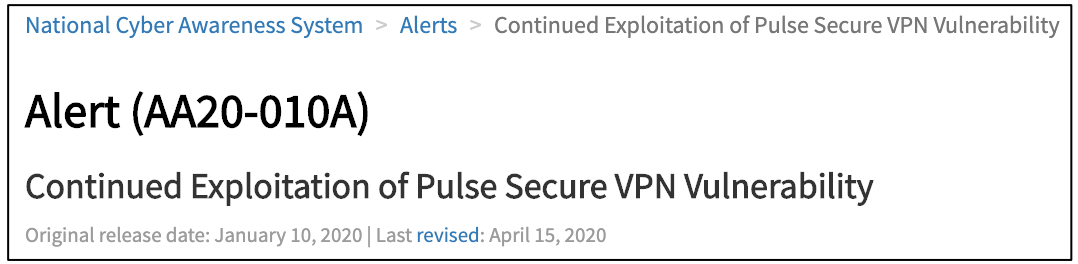

National Cyber Awareness System > Alerts > Ransomware Impacting Pipeline Operations

Alert (AA20-049A)

Ransomware Impacting Pipeline Operations

Original release date: February 18, 2020

- Alert AA20-049A
  - "A cyber threat actor used a Spearphishing Link to obtain initial access to the organization's information technology (IT) network before pivoting to its OT network."
  - "The threat actor then deployed commodity ransomware to Encrypt Data for Impact on both networks."


National Cyber Awareness System > Alerts > Continued Exploitation of Pulse Secure VPN Vulnerability

Alert (AA20-010A)

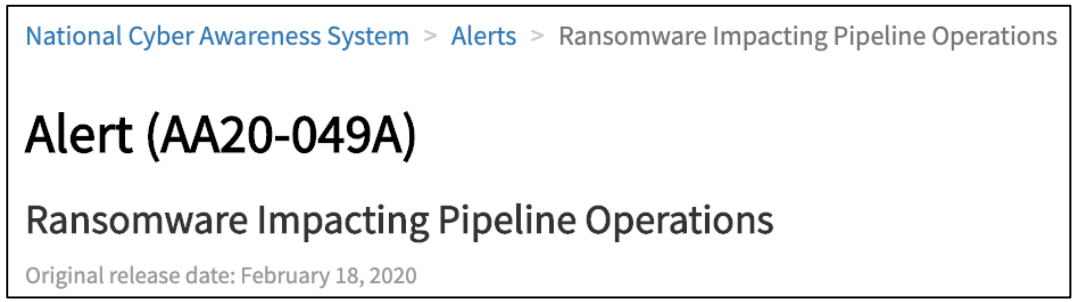
Continued Exploitation of Pulse Secure VPN Vulnerability

Original release date: January 10, 2020 | Last revised: April 15, 2020

- Alert AA20-01A
  - "October 16, 2019 – The CERT Coordination Center (CERT/CC) releases Vulnerability Note VU#927237: Pulse Secure VPN contains multiple vulnerabilities."
  - "January 2020 – Media reports cybercriminals now targeting unpatched Pulse Secure VPN servers to install REvil (Sodinokibi) ransomware."

Source: https://www.us-cert.gov/ncas/alerts/aa20-049a
Source: https://www.us-cert.gov/ncas/alerts/aa20-010a

OT Incident Response Plan Issues


National Cyber Awareness System > Alerts > Ransomware Impacting Pipeline Operations

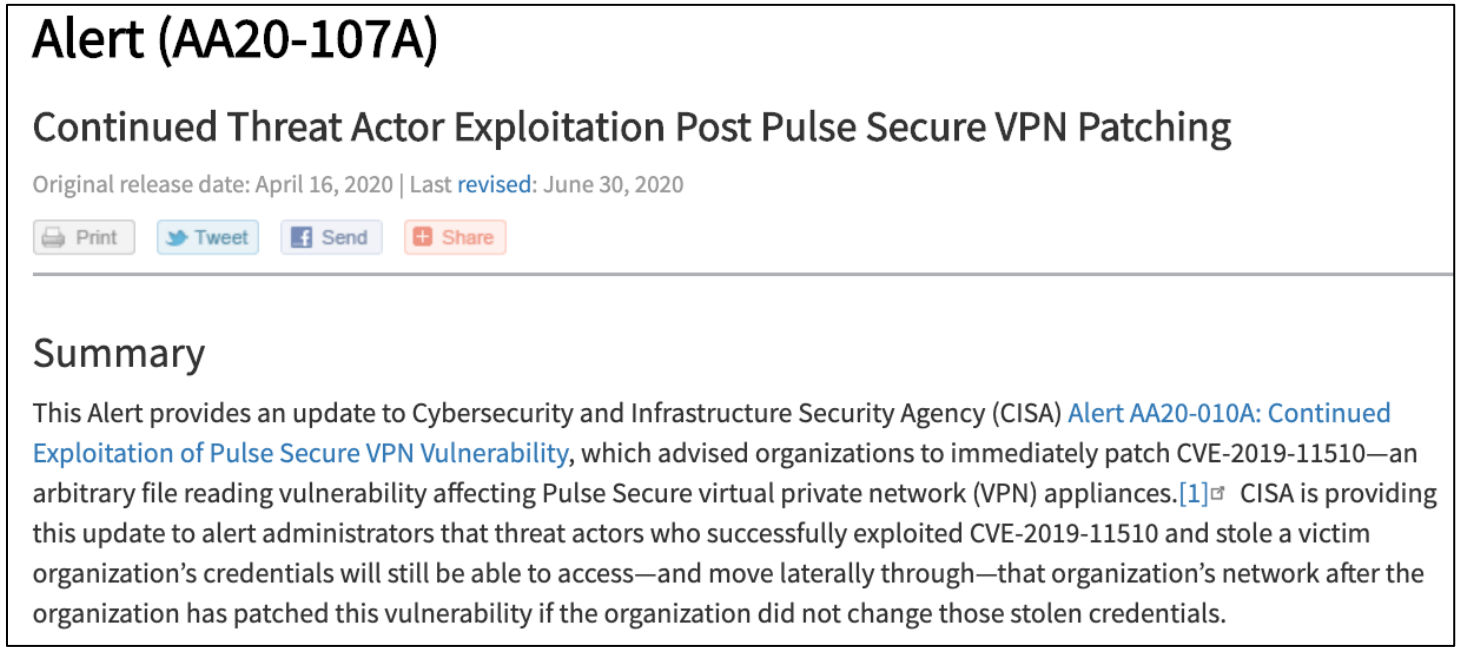
Alert (AA20-049A)

Ransomware Impacting Pipeline Operations

Original release date: February 18, 2020

"Although they considered a range of physical emergency scenarios, the victim's emergency response plan did not specifically consider the risk posed by cyberattacks. Consequently, emergency response exercises also failed to provide employees with decision-making experience in dealing with cyberattacks."

Gift That Keeps On Giving



Alert (AA20-107A)

Continued Threat Actor Exploitation Post Pulse Secure VPN Patching

Original release date: April 16, 2020 | Last revised: June 30, 2020

Print Tweet Send Share

Summary

This Alert provides an update to Cybersecurity and Infrastructure Security Agency (CISA) Alert AA20-010A: Continued Exploitation of Pulse Secure VPN Vulnerability, which advised organizations to immediately patch CVE-2019-11510—an arbitrary file reading vulnerability affecting Pulse Secure virtual private network (VPN) appliances.[1] CISA is providing this update to alert administrators that threat actors who successfully exploited CVE-2019-11510 and stole a victim organization's credentials will still be able to access—and move laterally through—that organization's network after the organization has patched this vulnerability if the organization did not change those stolen credentials.

- Attackers Exploit VPN Vulnerability
- Attackers Compromise Credentials
- Company Patches VPN
- Attackers Login with Compromised Credentials

Source: https://us-cert.cisa.gov/ncas/alerts/aa20-107a

SANS ICS IR White Paper

https://www.sans.org/reading-room/whitepapers/analyst/responding-incidents-industrial-control-systems-identifying-threats-reactions-developing-ir-process-39595

Self-Imposed Lack of Visibility

Table 6. OT/Control System Components Support of Visibility

OT/Control System Components	Risk	Impact	Collection
Server assets running commercial OS (Windows, UNIX, Linux)	57.6%	32.7%	73.6%
Network devices (firewall, switches, routers, gateways)	30.2%	30.2%	65.3%
Connections to other internal systems (enterprise networks, system to system) ★	42.0%	31.2%	54.4%
Engineering workstations	38.0%	29.3%	50.3%
Operator workstations	33.2%	28.8%	48.2%
Remote access appliances (VPN) ★	25.4%	18.5%	43.5%
Connections to the field control networks (SCADA) ★	36.1%	34.1%	38.9%
Physical access systems ★	22.4%	16.6%	30.6%
Control system communication protocols	23.9%	20.5%	28.0%
Wireless communication devices and protocols ★	27.8%	13.2%	27.5%
Process control application	16.1%	20.0%	21.2%
Plant historian	14.6%	13.2%	19.7%
Mobile devices (laptops, tablets, smartphones) ★	36.1%	12.2%	19.2%
Embedded controllers or components (e.g., PLCs, IEDs)	22.9%	33.2%	18.7%
Field devices (digital sensors and actuators)	19.5%	19.0%	13.5%
Analog modems ★	12.2%	6.3%	4.7%

- Red boxes identify the top four components by impact.
  - Less than half collect data from the most impactful devices.
- Red stars indicate components that provide external connectivity into the control network.
  - Less than half collect information from devices that provide remote access to their environments.

Realistic Security

"Prevention is ideal, but detection is a must."

Dr. Eric Cole, November 27, 2010

"...however, detection without response has minimal value."

SANS ICS410 ICS/SCADA Security Essentials

Team Table-Top Exercise Examples

Image Source: https://blog.zoom.us/wordpress/wp-content/uploads/2018/01/49-participants-view.gif

Don C. Weber - @cutaway

https://www.sans.org/profiles/don-c-weber/
https://www.cutawaysecurity.com/team/
https://www.linkedin.com/in/cutaway/