DRAGOS WORLDVIEW WEEK 11, 2021

08 - 14 March 2021

19 March 2021

TLP: AMBER FOR DRAGOS CUSTOMERS ONLY

Dragos WorldView Threat Intelligence summarizes and consolidates the major industrial control cybersecurity items during the last week. Dragos scores each item on its relevance and importance.

A limited threat, risk, or vulnerability requiring an applicability assessment before taking action

Questions? Submit a support request through the WorldView portal.

Contents

Suspect Domains 01 - 07 March 2021

10 March 2021

A limited threat, risk, or vulnerability requiring an applicability assessment before taking action

In total, Dragos identified 675 network items this period that either:

- Represent a potential threat to ICS owners by mimicking various ICS-related suppliers or other entities.
- Reflect more general threats by spoofing well-known IT services or organizations.
- Are general ICS themes that do not specifically indicate a malicious purpose other than acting as suspicious masquerades or enticing lures.

REFERENCE:

DOM-2021-10 – Suspect Domains 01 - 07 March 2021

WorldView Week 10, 2021 (01 - 07 March)

10 March 2021

A limited threat, risk, or vulnerability requiring an applicability assessment before taking action

Dragos published three intelligence reports: a report on PARISITE Pay2Key activity, Suspect Domains, and WorldView Weekly. Dragos assessed and corrected vulnerabilities in Schneider Electric, Rockwell Automation, and Hitachi ABB. Please review the report for corrections and mitigations.

REFERENCE:

WVW-2021-10 – WorldView Week 08 2021 (22 - 28 February)

Critical Infrastructure in India Targeted by Malware Campaign

08 March 2021

A limited threat, risk, or vulnerability requiring an applicability assessment before taking action

Dragos performed network telemetry flow analysis on the Indicators of Compromise (IOCs) provided by Recorded Future and confirmed many of the key findings in the report, *China-Linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions*. Dragos identified over 100 IP addresses in India that were recently, or currently, communicating over extended timeframes, with the 23 malware Command and Control (C2) IP addresses mentioned in the RedEcho report. Dragos also validated RedEcho infrastructure overlap in published literature, with threats tracked by FireEye as APT41, and Microsoft as BARIUM. While Dragos is unable to directly associate the RedEcho activity with any Activity Group (AG) tracked by Dragos, VANADANITE has overlapping power vertical victimology with RedEcho.

Concurrently, the New York Times published an article, *China Appears to Warn India: Push Too Hard and the Lights Could Go Out,* which references some of the findings of the Recorded Future report. The New York Times article implies that the October 2020 Mumbai, India power outage was a direct result of the RedEcho adversary purported to be sponsored by the Peoples Republic of China (PRC) government. At this time, Dragos does not support this conclusion given a lack of evidence.

REFERENCE:

Headlines

Updates on Microsoft Exchange Server Vulnerabilities

13 March 2021

A far-reaching threat or vulnerability calling for action broadly across at least one industry

Activity Group: N/A
Impacted Industries: All
Region: Worldwide
MITRE ATT&CK Techniques: Initial Access: Exploit Public-Facing Application [T1190], Persistence: Server Software Component: Web Shell [T1505.0003], Credential Access: Server Software Component: Web Shell [T1003.001]

On Saturday 13 March, the Cybersecurity and Infrastructure Security Agency (CISA) and the United States Computer Emergency Readiness Team (US-CERT) issued an update on the ongoing exploitation of Microsoft Exchange Server vulnerabilities. CISA added seven Malware Analysis Reports (MARs) to the original alert, AA21-062A.[1] The following malware reports were added:

- MAR-10328877-1.v1: China Chopper Webshell
- MAR-10328923-1.v1: China Chopper Webshell
- MAR-10329107-1.v1: China Chopper Webshell
- MAR-10329297-1.v1: China Chopper Webshell
- MAR-10329298-1.v1: China Chopper Webshell
- MAR-10329301-1.v1: China Chopper Webshell
- MAR-10329494-1.v1: China Chopper Webshell

While China Chopper is the primary webshell detailed by CISA, other webshells have been utilized. China Chopper is not conclusive for attributing exploitation to any one specific adversary.

Key Takeaway: CISA released MARs reports on the most widely used webshell in connection with the exploitation of Microsoft Exchange Server vulnerabilities. Open source information also indicates other webshells are being utilized. Organizations should be aware and follow recommendations to address this exploitation activity.

Recommendations:

- Follow Microsoft guidelines to immediately patch vulnerable Microsoft Exchange Servers.
- If an organization cannot patch immediately, temporarily disable external access to Microsoft Exchange.
- Follow Department of Homeland Security (DHS) and CISA guidelines for remediating Microsoft Exchange vulnerabilities.
- When checking for compromise by HAFIUM:
    - Scan Microsoft Exchange logs for indicators of compromise using the script provided on Microsoft's GitHub page.
    - Check root directory of web server for suspicious .aspx files.
    - Check for suspicious .zip, .rar, and .7z files in C:\ProgramData\, which may indicate possible data exfiltration.

[1] Alert (AA21-062A) – Cybersecurity & Infrastructure Security Agency

- Victims should monitor these paths for Local Security Authority Subsystem Service (LSASS) dumps: C:\windows\temp\ and C:\root.

REFERENCES:

Updates on Microsoft Exchange Server Vulnerabilities – Cybersecurity & Infrastructure Security Agency
Remediating Microsoft Exchange Vulnerabilities – Cybersecurity & Infrastructure Security Agency
Alert (AA21-062A) – Cybersecurity & Infrastructure Security Agency

Molson Coors Brewing Operations Impacted by Possible Ransomware Compromise

11 March 2021

A limited threat, risk, or vulnerability requiring an applicability assessment before taking action

Activity Group: N/A
Impacted Industries: Food and Beverage
Region: United States (U.S.)
MITRE ATT&CK Techniques: Impact: Data Encrypted for Impact [T1486]

On 11 March 2021, Molson Coors filed a Form 8-K with the SEC, disclosing that its operations were impacted by a network compromise. Open source information indicated that Molson Coors was impacted by ransomware of an unspecified type and attribution to a specific ransomware group. Dragos is not able to corroborate or confirm information that ransomware impacted Molson Coors, but it is highly probable that this occurred due to the breadth of disruption to Molson Coors' operations. As of Friday, 12 March 2021, sources reported that Molson Coors' operations were still not back online.

Presently, the details of the attack on the Molson Coors brewery are not fully known. However, this attack follows a pattern of recent attacks focused on manufacturing. Several of these ransomware attacks have happened just within the last month. For instance, the Spanish State Employment Service (SEPE) recently experienced a Ryuk ransomware attack, suspending its communications systems across hundreds of offices and delaying thousands of appointments. Kia Motors was disrupted by a ransomware attack in February where DoppelPaymer took credit. WestRock – the second-largest packaging company in the U.S., also had its business disrupted by a ransomware attack in February. Finnish IT giant TietoEVRY also was a victim of a ransomware attack last month, according to open source reporting.

Key Takeaway:

- The compromise halted control systems associated with brewery operations, production, and shipments.
- An unknown adversary almost certainly encrypted systems affecting brewery operations.
- It is unknown at this time if operations have resumed.

Recommendations:

- Apply the most up-to-date patches to Virtual Private Network (VPN) appliances to prevent exploitation of vulnerabilities against public facing infrastructure. This has become an increasingly favored tactic for ransomware groups.
- Verify security between business IT networks and operational technology networks. Reinforce defense in depth policies across security enclaves and domains that service IT and OT functions. Redefine vendor roles in extant OT enclaves within the organization. Carefully vet and verify any employee or vendor with remote access to OT layers of the organization
- Reinforce internal policies and education regarding suspicious emails. Verify and check emails before clicking links, and alert email service providers or onsite personnel to be aware of spearphishing attacks.

- Deploy automated software update tools to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.
- Use up-to-date and trusted third-party components for the software developed by the organization.
- Add additional security controls to prevent the access from unauthenticated sources.

REFERENCE:

Molson Coors brewing operations disrupted by cyberattack – Bleeping Computer

Ransomware Roundup

Ransomware attacks are increasingly targeting and compromising industrial companies globally, often disrupting operations. Dragos monitors multiple dark web "leak sites" where ransomware adversaries claim to post stolen data of the alleged victims. This section provides a list of ransomware targeting industrial and related entities, overviews of known compromises, and defensive recommendations.

Ransomware Being Used in Conjunction with Recent Microsoft Exchange Server Vulnerabilities

11 March 2021

Items of interest but likely requiring no action except in unique threat models

An unknown adversary began utilizing previously compromised Microsoft Exchange Servers to deploy a new ransomware strain called DearCry. DearCry creates a Windows service named "msupdate" that performs the encryption effect. The service is stopped, then removed after the encryption process is completed. Files encrypted by DearCry get prepended with a 'DEARCRY!' string.

REFERENCES:

Cybersecurity firm Qualys seems to have suffered a data breach, threat actors allegedly exploited zero-day flaw in their Accellion FTA server – Security Affairs
Cybersecurity firm Qualys is the latest victim of Accellion hacks – Bleeping Computer
Mandiant validates full remediation of all known security vulnerabilities in the FTA product – Accellion
Alert (AA21-055A): Exploitation of Accellion File Transfer Appliance – Cybersecurity & Infrastructure Security Agency

Recommendations:

- Follow Microsoft guidance to patch Exchange Server software.
- If immediate patching is not possible, follow DHS and CISA mitigation guidelines for organizations with Microsoft Exchange Servers.
- General recommendations for ransomware:
  - Ensure employees are trained to recognize phishing campaigns and report them to security personnel.
  - Implement flagging or other methods to tag external email and mitigate internal email address spoofing.
  - Disable macros in Microsoft Office applications.
  - Keep antivirus signatures up-to-date, where possible.
  - Ensure software and hardware are kept up-to-date and implement upgrades as soon as practical.
  - Block internet access to and from control system assets.
  - Ensure corporate networks are thoroughly patched to prevent malware infections targeting disclosed vulnerabilities from entering the environment and prevent subsequent propagation that may impact ICS networks.

- Critically examine and limit connections, including network shares between corporate and ICS networks, to only required traffic.
- Mandate Multi-Factor Authentication (MFA) for all remote access mechanisms, including Remote Desktop Protocol (RDP).
- Maintain backups of Information Technology (IT) and Operational Technology (OT) network systems.
- Test backups during a disaster recovery simulation.
- Leverage industrial-specific threat detection mechanisms to identify malware within OT and reinforce defense in depth strategies at the network level.
- Ensure strong network defenses between IT and OT networks to create chokepoints to limit malware spread.
- Only allow Wake-on-Lan packets to be received from administrative devices and workstations.

Vulnerability Advisories

11 This week, independent Dragos analysis identified 11 individual vulnerabilities (CVEs) with incorrect data a 42 percent error rate. Two of the 26 were found to be more severe, six of the 26 were found to be less severe, and three of the 26 were found to have the same score but different prerequisites and outputs from exploitation. The correct data are included in the advisories below.

Siemens SCALANCE and SIMATIC libcurl

09 March 2021

A limited threat, risk, or vulnerability requiring an applicability assessment before taking action

Siemens SCALANCE SC600 and SIMATIC NET CM are a security appliance and communication module deployed worldwide and commonly seen in multiple industrial sectors.

Key Takeaways:

- There is a vulnerability in Siemens' SCALANCE SC600 and SIMATIC NET CM 1542-1 that could allow an adversary to deny availability to the systems or execute code.
- An unauthenticated and remote adversary could cause a Denial of Service (DoS) condition or execute code and take control of the devices.
- Restrict access to ports TCP/25, TCP/80, or TCP/443.

Note:
The ICS-CERT advisory does not include several other notable vulnerabilities, including CVE-2018-14618, CVE-2018-16890, CVE-2019-3822, and CVE-2019-6570.
CVE-2018-14618 appears to have an incorrect CVSS. Dragos assesses that the score should be:
7.5 => **9.8**
AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H => AV:N/***AC:L***/PR:N/***UI:N***/S:U/C:H/I:H/A:H
CVE-2018-16890 appears to have an incorrect CVSS. Dragos assesses that the score should be:
7.5 => **5.3**
AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H => AV:N/***AC:H***/PR:N/***UI:R***/S:U/C:N/I:N/A:H
CVE-2019-3822 appears to have an incorrect CVSS. Dragos assesses that the score should be:
8.1 => **9.8**
AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H => AV:N/***AC:L***/PR:N/UI:N/S:U/C:H/I:H/A:H

Siemens SCALANCE and SIMATIC libcurl
Date: 09 March 2021
Source: ICS-CERT
CVE-2018-14618
CVE-2018-16890
CVE-2019-3822
CVE-2019-3823
CVE-2019-6570

Dragos Assessment
Restrict access to ports TCP/25, TCP/80, or TCP/443.

Patch/Defense Details
Update SCALANCE SC600 firmware to a patched version, v2.0 or later.

Attributes	
Active Exploitation	No
Skill Level Required	Low
Access Level Required	
Remotely Exploitable	✓
Physical Access Required	
Known Credentials	
User Interaction	
Security Impact	
Denial of Service	✓
Credential Exposure	
Code Execution/Modify App	✓
Broader Network Access	
Privilege Escalation	
Data Theft/Data Tamper	✓

Description
Successful exploitation of this third-party vulnerability could allow an adversary to cause a Denial of Service (DoS) condition or execute code and take control of the systems.

Affecting
- SCALANCE SC600 Family: all versions prior to v2.0.
- SIMATIC NET CM 1542-1: all versions.

Additional Resources
Siemens Security Advisory: SSA-436177
ICSA-21-068-10

Disable the Simple Mail Transfer Protocol (SMTP) client function if possible.	**Operation Impact** Loss of View Loss of Control	

Siemens SINEMA Remote Connect Server

09 March 2021

A limited threat, risk, or vulnerability requiring an applicability assessment before taking action

Siemens' SINEMA Remote Connect Server is a remote network access system deployed worldwide and commonly seen in the critical manufacturing industry.

Key Takeaways:

- There are vulnerabilities in Siemens' SINEMA Remote Connect Server that could allow an adversary to bypass authentication.
- A locally authenticated but unprivileged adversary could view sensitive information or modify authentication server configuration files.
- Restrict access to port TCP/443.

Siemens SINEMA Remote Connect Server
Date: 09 March 2021
Source: ICS-CERT
CVE-2020-25239
CVE-2020-25240

Dragos Assessment
Restrict access to port TCP/443.

Patch/Defense Details
Update to a patched version, v3.0 or later.

Attributes	
Active Exploitation	No
Skill Level Required	Low
Access Level Required	
Remotely Exploitable	✓
Physical Access Required	
Known Credentials	✓
User Interaction	
Security Impact	
Denial of Service	✓
Credential Exposure	
Code Execution/Modify App	✓
Broader Network Access	
Privilege Escalation	
Data Theft/Data Tamper	✓
Operation Impact	
Loss of View	
Loss of Control	

Description
Successful exploitation of these vulnerabilities could allow authenticated, unprivileged user accounts to access unauthorized functionality.

Affecting
- SINEMA Remote Connect Server: All versions prior to v3.0

Additional Resources
Siemens Security Advisory: SSA-731317
ICSA-21-068-04

Siemens SCALANCE and RUGGEDCOM Devices Secure Shell (SSH)

09 March 2021

A limited threat, risk, or vulnerability requiring an applicability assessment before taking action

Siemens' SCALANCE and RUGGEDCOM product lines are industrial networking devices deployed worldwide and commonly seen across multiple industrial sectors.

Key Takeaways:

- There is a vulnerability in Siemens' SCALANCE and RUGGEDCOM devices that could allow an adversary to deny availability to the device.
- An unauthenticated and remote adversary could cause a Denial of Service (DoS) condition in the device when attempting to authenticate multiple times, forcing the device to reboot.
- Restrict access to port TCP/22. Ensure the SSH service is not accessible on the open internet.

Siemens SCALANCE and RUGGEDCOM Devices SSH
Date: 09 March 2021
Source: ICS-CERT
CVE-2021-25676

Dragos Assessment
Restrict access to port TCP/22. Ensure the SSH service is not accessible on the open internet.

Patch/Defense Details
Update to a patched version:

- SCALANCE SC-600: update to v2.1.3 or later.

Siemens' has not yet released patches to address this issue for devices other than SCALANCE SC-600.

Attributes	
Active Exploitation	No
Skill Level Required	Low
Access Level Required	
Remotely Exploitable	✓
Physical Access Required	
Known Credentials	
User Interaction	
Security Impact	
Denial of Service	✓
Credential Exposure	
Code Execution/Modify App	
Broader Network Access	
Privilege Escalation	
Data Theft/Data Tamper	
Operation Impact	
Loss of View	✓
Loss of Control	✓

Description
Successful exploitation allows an unauthenticated and remote adversary to cause a DoS condition and force the device to reboot.

Affecting

- RUGGEDCOM RM1224: v6.3
- SCALANCE M-800: v6.3
- SCALANCE: S615: v6.3
- SCALANCE SC-600: All versions from v2.1 and prior to v2.1.3

Additional Resources
Siemens Security Advisory: SSA-296266
ICSA-21-068-02

Schneider Electric IGSS SCADA Software

11 March 2021

Threat scenarios, research, and vulnerabilities relating to operations but not requiring direct/immediate action

Schneider Electric's Interactive Graphical SCADA System (IGSS) is a full featured automation software deployed worldwide and commonly seen in commercial facilities, critical manufacturing, and energy industries.

Key Takeaways:

- There are vulnerabilities in Schneider Electric's IGSS that could allow an adversary to execute code.
- An unauthenticated and remote adversary could execute code and take control of the host system if they can trick an authenticated user into loading a malicious project file into the application.
- Train users to only load project files from known and trusted sources, especially of type .cgf. Ensure the IGSS system is not directly accessible on the open internet.

Schneider Electric IGSS SCADA Software	**Attributes**		**Description**
Date: 11 March 2021	Active Exploitation	No	Successful exploitation of these vulnerabilities allows an unauthenticated and remote adversary to take control of the host system if they can trick an authenticated user into loading a malicious .cgf project file.
Source: ICS-CERT	Skill Level Required	Low	
CVE-2021-22709			
CVE-2021-22710	**Access Level Required**		
CVE-2021-22711	Remotely Exploitable	✓	
CVE-2021-22712	Physical Access Required		
	Known Credentials		
Dragos Assessment	User Interaction	✓	**Affecting**
Train users to only load project files from known and trusted sources, especially of type .cgf. Ensure the IGSS system is not directly accessible on the open internet.	**Security Impact**		• IGSS Definition: v15.0.0.21041 and prior.
	Denial of Service	✓	
Patch/Defense Details	Credential Exposure		**Additional Resources**
Update to a patched version, v15.0.0.21042 or later.	Code Execution/Modify App	✓	Schneider Electric's Security Advisory: SEVD-2021-068-01
	Broader Network Access		ICSA-21-070-01
	Privilege Escalation		
	Data Theft/Data Tamper	✓	
	Operation Impact		
	Loss of View	✓	
	Loss of Control	✓	

Siemens Solid Edge File Parsing

09 March 2021

Threat scenarios, research, and vulnerabilities relating to operations but not requiring direct/immediate action

Siemens' Solid Edge is a collection of 3D Computer Aided Design (CAD) modeling software deployed worldwide and commonly seen in the critical manufacturing industry.

Key Takeaways:

- There are vulnerabilities in Siemens' Solid Edge that could allow an adversary to deny availability to the software or execute code on the host system.
- A locally authenticated adversary could crash the software or take control of the host system and execute code if they can trick an authenticated user into loading a malicious project file.
- Train users to only load files into the application from trusted sources, especially of type .par, .xml, and .dft. Ensure engineering workstations are not directly connected to the internet.

Note:
CVE-2020-28387 appears to have an incorrect CVSS. Dragos assesses that the score should be:
5.6 => **5**
AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:L => AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/***A:N***

Siemens Solid Edge File Parsing
Date: 09 March 2021
Source: ICS-CERT
CVE-2020-28385
CVE-2020-28387
CVE-2021-27380
CVE-2021-27381

Dragos Assessment
Train users to only load files into the application from trusted sources, especially of type .par, .xml, and .dft. Ensure engineering workstations are not directly connected to the internet.

Patch/Defense Details
Update to a patched version (or later):

- Solid Edge SE2020: Update to SE2020MP13 or later (login required)
- Solid Edge SE2021: Update to SE2021MP3 or later (login required). This only mitigates CVE-2020-28387 and CVE-2021-27381.

Attributes	
Active Exploitation	No
Skill Level Required	Low
Access Level Required	
Remotely Exploitable	✓
Physical Access Required	
Known Credentials	
User Interaction	✓
Security Impact	
Denial of Service	✓
Credential Exposure	
Code Execution/Modify App	✓
Broader Network Access	
Privilege Escalation	
Data Theft/Data Tamper	✓
Operation Impact	
Loss of View	
Loss of Control	

Description
Successful exploitation of these vulnerabilities could lead to a DoS condition, and could lead to arbitrary code execution or data exfiltration on the host system.

Affecting

- Solid Edge SE2020: All versions before SE2020MP13.
- Solid Edge SE2021: version SE2021MP3 and prior.

Additional Resources
ICSA-21-068-09

Siemens SENTRON PAC and 3VA Devices

09 March 2021

Threat scenarios, research, and vulnerabilities relating to operations but not requiring direct/immediate action

Siemens' SENTRON PAC are a family of power measuring devices. SENTRON 3VA DSP800 is a display device for the 3VA MCCB. SENTRON 3VA COM100/800 are data servers used as a gateway between the 3VA MCCB and other automation systems. They are all displayed worldwide and commonly seen in the energy industry.

Key Takeaways:

- There are vulnerabilities in Siemens' SENTRON 3VA and PAC devices, nicknamed AMNESIA:33, that could allow an adversary to deny availability to the systems.
- These vulnerabilities allow an adversary with access to the Local Area Network (LAN) to send a specially crafted packet and cause a DoS condition in the device.
- Ensure logging is enabled and monitor network endpoints for suspicious or unfamiliar connections. These devices should not be accessible from the open internet.

Note:
These two vulnerabilities were first reported in 2020 by ForeScout and nicknamed AMNESIA:33.
CVE-2020-13987 appears to have an incorrect CVSS. Dragos assesses that the score should be:
8.2 => **7.5**
AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H => AV:N/AC:L/PR:N/UI:N/S:U/C:N/***I:N***/A:H
CVE-2020-17437 appears to have an incorrect CVSS. Dragos assesses that the score should be:
8.2 => **7.5**
AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H => AV:N/AC:L/PR:N/UI:N/S:U/***C:N***/I:N/A:H

Siemens SENTRON PAC and 3VA Devices Date: 09 March 2021 Source: ICS-CERT CVE-2020-13987 CVE-2020-17437 **Dragos Assessment** Ensure logging is enabled and monitor network endpoints for suspicious or unfamiliar connections. These devices should not be accessible from the open internet. **Patch/Defense Details** Update to a patched version: • SENTRON PAC3200: Update to v2.4.7 or later version. • SENTRON PAC3220: Update to v3.2.0 or later version. Contact Siemens customer support to receive the latest firmware version.	**Attributes**		**Description** Successful exploitation of these vulnerabilities could cause a DoS condition. **Affecting** • SENTRON 3VA COM100/800: all versions. • SENTRON 3VA DSP800: all versions. • SENTRON PAC2200 (with CLP Approval): all versions. • SENTRON PAC2200 (with MID Approval): all versions. • SENTRON PAC2200 (without MID Approval): all versions. • SENTRON PAC3200: prior to v2.4.7. • SENTRON PAC3200T: all versions. • SENTRON PAC3220: prior to v3.2.0.
	Active Exploitation	No	
	Skill Level Required	Low	
	Access Level Required		
	Remotely Exploitable		
	Physical Access Required		
	Known Credentials		
	User Interaction		
	Security Impact		
	Denial of Service	✓	
	Credential Exposure		
	Code Execution/Modify App		
	Broader Network Access		
	Privilege Escalation		
	Data Theft/Data Tamper		
	Operation Impact		
	Loss of View	✓	
	Loss of Control	✓	

• SENTRON PAC4200: Update to v2.3.0 or later version. SENTRON 3VA COM100/800, 3VA DSP800, PAC2200, and PAC3200T do not have a patch available to address these issues.		• SENTRON PAC4200: prior to v2.3.0. **Additional Resources** Siemens Security Advisory: SSA-541018 ICSA-21-068-06

Siemens LOGO! 8 BM

09 March 2021

Threat scenarios, research, and vulnerabilities relating to operations but not requiring direct/immediate action

Siemens' LOGO! 8 BM is a Programmable Logic Controller (PLC) deployed worldwide and commonly seen in the commercial facilities and transportation system industries.

Key Takeaways:

- There is a vulnerability in Siemens' LOGO! 8 BM that could allow an adversary to deny availability to the PLC.
- An unauthenticated and remote adversary could cause a DoS condition in the device if they can trick an authenticated user into loading a malicious project file. A manual reset of the device is required to resume normal operations.
- Train users to only load project files into the application from known and trusted sources. Ensure PLCs are not directly accessible from the internet.

Siemens LOGO! 8 BM
Date: 09 March 2021
Source: ICS-CERT
CVE-2020-25236

Dragos Assessment
Train users to only load project files into the application from known and trusted sources. Ensure PLCs are not directly accessible from the internet.

Patch/Defense Details
Siemens has not yet produced a patch to address this issue.

Attributes	
Active Exploitation	No
Skill Level Required	Low
Access Level Required	
Remotely Exploitable	✓
Physical Access Required	
Known Credentials	
User Interaction	✓
Security Impact	
Denial of Service	✓
Credential Exposure	
Code Execution/Modify App	
Broader Network Access	
Privilege Escalation	
Data Theft/Data Tamper	
Operation Impact	
Loss of View	✓
Loss of Control	✓

Description
Successful exploitation of this vulnerability could allow an adversary to cause a DoS condition if a user is tricked into loading a malicious project file.

Affecting
- LOGO! 8 BM (incl. SIPLUS variants): All versions

Additional Resources
Siemens Security Advisory: SSA-783481
ICSA-21-068-05

Siemens SCALANCE and RUGGEDCOM Devices

09 March 2021

Threat scenarios, research, and vulnerabilities relating to operations but not requiring direct/immediate action

Siemens' SCALANCE and RUGGEDCOM product lines are industrial networking devices deployed worldwide and commonly seen across multiple industrial sectors.

Key Takeaways:

- There is a vulnerability in Siemens' SCALANCE and RUGGEDCOM systems that could allow an adversary to deny availability or potentially execute code.
- An adversary with access to the Local Area Network (LAN) could cause a DoS condition in the device and force a reboot. Code execution is possible under special conditions.
- Deactivate the STP passive listening feature, which completely mitigates this issue.

Siemens SCALANCE and RUGGEDCOM Devices
Date: 09 March 2021
Source: ICS-CERT
CVE-2021-25667

Dragos Assessment
Deactivate the STP passive listening feature, which completely mitigates this issue.

Patch/Defense Details
Update to a patched version:

- SCALANCE SC-600 Family: Update to v2.1.3 or later.
- SCALANCE X300WG: Update to v4.1 or later.
- SCALANCE XM400: Update to v6.2 or later.
- SCALANCE XR500: Update to v6.2 or later.
- SCALANCE Xx200 Family: Update to v4.1 or later.

Attributes	
Active Exploitation	No
Skill Level Required	Low
Access Level Required	
Remotely Exploitable	
Physical Access Required	
Known Credentials	
User Interaction	
Security Impact	
Denial of Service	✓
Credential Exposure	
Code Execution/Modify App	✓
Broader Network Access	
Privilege Escalation	
Data Theft/Data Tamper	✓
Operation Impact	
Loss of View	✓
Loss of Control	✓

Description
Successful exploitation could allow an unauthenticated and remote adversary with access to the LAN to force the device to reboot. Code execution is possible under special conditions.

Affecting

- RUGGEDCOM RM1224: All versions v4.3 and later.
- SCALANCE M-800: All versions v4.3 and later.
- SCALANCE S615: All versions v4.3 and later.
- SCALANCE SC-600 Family: All versions from v2.0 and prior to v2.1.3.
- SCALANCE X300WG: All versions prior to v4.1.
- SCALANCE XM400: All versions prior to v6.2.
- SCALANCE XR500: All versions prior to v6.2.
- SCALANCE Xx200 Family: All versions prior to v4.1.

Additional Resources
Siemens Security Advisory: SSA-979775
ICSA-21-068-03

Siemens SIMATIC S7-PLCSIM

09 March 2021

Threat scenarios, research, and vulnerabilities relating to operations but not requiring direct/immediate action

Siemens' SIMATIC S7-PLCSIM is software for simulating controllers such as the S7-1500 and ET 200 SP. It is deployed worldwide and seen across multiple industrial sectors.

Key Takeaways:

- There is a vulnerability in Siemens' SIMATIC S7-PLCSIM that could allow an adversary to deny availability to the system.
- An adversary could cause a DoS condition in the application and force a crash by tricking a user into loading a malicious project file. The service must be restarted to resume normal operations.
- Train users to only load project files into the application from trusted sources. Ensure engineering workstations are not directly connected to the internet.

Note:
CVE-2021-25673 appears to have an incorrect CVSS. Dragos assesses that the score should be:
5.5 => **5.5**
AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H => AV:L/AC:L/***PR:N***/***UI:R***/S:U/C:N/I:N/A:H
CVE-2021-25674 appears to have an incorrect CVSS. Dragos assesses that the score should be:
5.5 => **5.5**
AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H => AV:L/AC:L/***PR:N***/***UI:R***/S:U/C:N/I:N/A:H
CVE-2021-25675 appears to have an incorrect CVSS. Dragos assesses that the score should be:
5.5 => **5.5**
AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H => AV:L/AC:L/***PR:N***/***UI:R***/S:U/C:N/I:N/A:H

Siemens SIMATIC S7-PLCSIM

Date: 09 March 2021
Source: ICS-CERT
CVE-2021-25673
CVE-2021-25674
CVE-2021-25675

Dragos Assessment
Train users to only load project files into the application from trusted sources. Ensure engineering workstations are not directly connected to the internet.

Patch/Defense Details
Siemens has not yet released a patch to address this issue.

Attributes	
Active Exploitation	No
Skill Level Required	Low
Access Level Required	
Remotely Exploitable	✓
Physical Access Required	
Known Credentials	
User Interaction	✓
Security Impact	
Denial of Service	✓
Credential Exposure	
Code Execution/Modify App	
Broader Network Access	
Privilege Escalation	
Data Theft/Data Tamper	
Operation Impact	
Loss of View	
Loss of Control	

Description
Successful exploitation of these vulnerabilities allows an adversary to crash the application by tricking an authenticated user into loading a malicious project file. The service will need to be restarted to recover and resume normal operations.

Affecting
- SIMATICS S7-PLCSIM v5.4: All versions.

Additional Resources
Siemens Security Advisory: SSA-256092
ICSA-21-068-01

Siemens Energy PLUSCONTROL 1st Gen

09 March 2021

Items of interest but likely requiring no action except in unique threat models

Siemens' PLUSCONTROL products are control devices for high power energy transmission with modular multilevel converters

Key Takeaways:

- There is a vulnerability in Siemens' Energy PLUSCONTROL that could allow an adversary to deny availability or potentially insert traffic into established connections.
- A remote and unauthenticated adversary can deny communication of PLUSCONTROL or potentially insert traffic into existing TCP connections.
- Dragos assesses this vulnerability does not pose an immediate risk to control systems. Ensure network segmentation is in place and PLUSCONTROL is not directly accessible on the internet.

Note:
This vulnerability is one of multiple in a set of vulnerabilities nicknamed NUMBER:JACK.
CVE-2020-28388 appears to have an incorrect CVSS. Dragos assesses that the score should be:
6.5 => **4.8**
AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L => AV:N/***AC:H***/PR:N/UI:N/S:U/C:N/I:L/A:L

Siemens Energy PLUSCONTROL 1st Gen
Date: 09 March 2021
Source: ICS-CERT
CVE-2020-28388

Dragos Assessment
Dragos' assesses this vulnerability does not pose an immediate or serious risk to control systems. Ensure network segmentation is in place and PLUSCONTROL is not directly accessible on the internet.

Patch/Defense Details
Siemens' has not yet released a patch to address this issue.

Attributes	
Active Exploitation	No
Skill Level Required	Low
Access Level Required	
Remotely Exploitable	✓
Physical Access Required	
Known Credentials	
User Interaction	
Security Impact	
Denial of Service	✓
Credential Exposure	
Code Execution/Modify App	
Broader Network Access	
Privilege Escalation	
Data Theft/Data Tamper	✓
Operation Impact	
Loss of View	
Loss of Control	

Description
Successful exploitation of this vulnerability could affect integrity of TCP connections.

Affecting
- PLUSCONTROL 1st Gen: all versions

Additional Resources
Siemens' Security Advisory: SSA-344238
ICSA-21-068-08

Siemens TCP Stack of SIMATIC MV400

09 March 2021

Items of interest but likely requiring no action except in unique threat models

Siemens' SIMATIC MV400 is an optical code reader for automatic identification of goods and materials. It is deployed worldwide and commonly seen in the critical manufacturing industry.

Key Takeaways:

- There are vulnerabilities in the TCP stack of Siemens' SIMATIC MV400 that could allow an adversary to deny communication or potentially spoof TCP sessions and inject data into the system.
- An unauthenticated and remote adversary could terminate existing TCP sessions by sending a TCP RST packet, or potentially spoof TCP sessions and send a crafted packet.
- Dragos assesses this vulnerability does not pose an immediate risk to control systems. Ensure proper network segmentation is in place and use a VPN when possible.

Note:
CVE-2020-27632 is one of multiple in a set of vulnerabilities nicknamed NUMBER:JACK.
CVE-2020-27632 appears to have an incorrect CVSS. Dragos assesses that the score should be:
7.5 => **4.8**
AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N => AV:N/***AC:H***/PR:N/UI:N/S:U/C:N/***I:L***/***A:L***

Siemens TCP Stack of SIMATIC MV400
Date: 09 March 2021
Source: ICS-CERT
CVE-2020-25241
CVE-2020-27632

Dragos Assessment
Dragos assesses this vulnerability does not pose an immediate or serious risk to control systems. Ensure proper network segmentation is in place and use a VPN when possible.

Patch/Defense Details
Update firmware to a patched version, v7.0.6 or later.

Attributes	
Active Exploitation	No
Skill Level Required	Low
Access Level Required	
Remotely Exploitable	✓
Physical Access Required	
Known Credentials	
User Interaction	
Security Impact	
Denial of Service	✓
Credential Exposure	
Code Execution/Modify App	
Broader Network Access	
Privilege Escalation	
Data Theft/Data Tamper	✓
Operation Impact	
Loss of View	
Loss of Control	

Description
Successful exploitation of these vulnerabilities could cause a DoS condition or affect the integrity of TCP connections.

Affecting
- SIMATIC MV400 family: prior to v7.0.6

Additional Resources
Siemens' Security Advisory: SSA-599268
ICSA-21-068-07