DRAGOS WORLDVIEW WEEK 44, 2022
27 October – 2 November

02 November 2022

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 requires an applicability assessment before taking action.

Questions? Submit a support request through the WorldView portal. Previous Worldview Weeks are accessible here by filtering for Worldview Weekly under Report Type.

Contents

Dragos Intelligence

Suspect Domains 24 October – 30 October 2022

02 November

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

In total, Dragos identified 384 network items this period that either:

- Represent a potential threat to owners of Industrial Control Systems (ICS) by mimicking various ICS-related suppliers or other entities.
- Reflect more general threats by spoofing well-known Information Technology (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?

These general ICS themes do not indicate a malicious purpose other than acting as suspicious masquerades or enticing lures.

REFERENCE:
DOM-2022-44: Suspect Domains 24 October – 30 October 2022 – Dragos

Another Hacktivist Group Continues Disruptive Attacks in Russia

01 November

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

Active since June 2022, the pro-Ukrainian hacktivists group, OneFist, is the second known hacktivist group to target industrial infrastructure in Russia. Dragos obtained information from a trusted source that OneFist is targeting any industrial infrastructure that supports Russian military operations in response to the Russia-Ukraine Conflict. Dragos assesses with moderate confidence that OneFist will continue targeting industrial infrastructure in Russia as long as the Ukraine-Russia Conflict continues. Dragos will continue to monitor OneFist's activity and provide further updates as needed.

REFERENCE:
AA-2022-45: Another Hacktivist Group Continues Disruptive Attacks in Russia – Dragos

Headlines

Major German Energy Supplier Hit by Cyber Attack

27 October

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

Enercity, one of Germany's largest municipal energy suppliers, confirmed it was targeted by a cyberattack on Wednesday morning. Enercity confirmed that it would continue supplying energy to customers, explaining that its operational technology and critical industrial infrastructure were not affected. However, the attack has impacted customer service, which has limited availability. The company added: "Not all IT systems can currently be used to their full extent."

Criminals have repeatedly targeted the energy sector in Germany has been in recent months. Several cyber incidents preceding the Russian invasion of Ukraine in February affected the oil and chemical sector in the country and neighboring countries, provoking public concerns that they were part of a criminal campaign coordinated by Russian intelligence. Additionally, indictments against Russian cybercriminals have alleged that Russia's Federal Security Service has at times, turned to domestic cyber criminals for foreign operations.

REFERENCE:
Major German energy supplier hit by cyberattack – The Record

White House Launches Chemical Sector Security Sprint

27 October

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

The Biden–Harris administration has launched a new initiative designed to improve the security of industrial systems in the chemical sector over the next 100 days, as part of ongoing efforts to reduce cyber-risk in critical infrastructure (CNI). The sector is the fourth to be covered by the Industrial Control Systems (ICS) Cybersecurity Initiative, following similar initiatives in the electricity, pipeline, water, and railway industries. Incorporating lessons learned from those previous efforts, the100-day security "sprint" will focus on:

- Information sharing and coordination between the federal government and the private sector
- Prioritizing "high-risk chemical facilities" that "present significant chemical release hazards"

The goal is to disseminate best practices for enhanced ICS cybersecurity across the entire chemical sector, which impacts other critical sectors, including manufacturing, healthcare, and fuel, among others.

REFERENCE:
White House Launches Chemical Sector Security Sprint - Infosecurity Magazine
White House Launches Chemical Sector Security Sprint – The Record

DHS Develops Baseline Cybersecurity Goals for Critical Infrastructure

28 October

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

The DHS on Thursday announced Cybersecurity Performance Goals (CPGs) to help organizations — particularly in critical infrastructure sectors — prioritize cybersecurity investments and address critical risks. The CPGs were developed by the DHS's Cybersecurity and Infrastructure Security Agency (CISA) in collaboration with the National Institute of Standards and Technology (NIST) based on feedback from partners in public and private sectors. They result from the White House's efforts to improve the US' cybersecurity. The DHS says the goals are unique in that they address

risk not only to individual entities but also the aggregate risk to the nation. CPGs are a set of cross-sector recommendations that can be highly useful to an organization in securing its systems, but they are voluntary — the government does not require organizations to use them. They are designed to complement NIST's Cybersecurity Framework. CPG categories include account security, device security, data security, governance and training, vulnerability management, supply chain / third party, and response and recovery.

REFERENCE:
DHS Develops Baseline Cybersecurity Goals for Critical Infrastructure – SecurityWeek

CISA: Understanding and Responding to Distributed Denial-of-Service Attacks

28 October

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

The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) are releasing this a joint guide to provide organizations with proactive steps to reduce the likelihood and impact of distributed denial-of-service (DDoS) attacks. These attacks can cost an organization time and money and may impose reputational costs while resources and services are inaccessible. Denial-of-service (DoS) attacks are a type of cyberattack targeting a specific application or website with the goal of exhausting the target system's resources, which, in turn, renders the target unreachable or inaccessible, denying legitimate users access to the service.

REFERENCE:
CISA: Understanding and Responding to Distributed Denial-of-Service Attacks - CISA
CISA, FBI, MS-ISAC Publish Guidelines For Federal Agencies on DDoS Attacks - Infosecurity Magazine

Largest EU Copper Producer Aurubis Suffers Cyberattack, IT Outage

28 October

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

German copper producer Aurubis has announced that it suffered a cyberattack that forced it to shut down IT systems to prevent the attack's spread. Aurubis is Europe's largest copper producer and the second largest in the world, with 6,900 employees worldwide, and produces one million tons of copper cathodes yearly. Aurubis said in a statement that they shut down various systems at their locations but that this has not impacted production. According to Aurubis' announcement, "The production and environmental protection facilities at the smelter sites are running, and incoming and outgoing goods are also being maintained manually."

Some operations have turned to manual mode to keep the flow of incoming and outgoing goods adequate for as long as required until computer-assisted automation returns at the smelters. Aurubis states that it's impossible to estimate how long it will take for all its systems to return to normal operations. Aurubis says the attack was "part of a larger attack on the metals and mining industry." The last time such a large metal producer was hit by ransomware was in March 2019, when LockerGoga forced aluminum giant Norsk Hydro to shut down its IT systems. Customers and suppliers can still reach their Aurubis contacts by phone.

REFERENCE:
Largest EU copper producer Aurubis suffers cyberattack, IT outage – BleepingComputer
Europe's Biggest Copper Producer Hit by Cyber-Attack - Infosecurity Magazine

CISA Unveils Cybersecurity Goals For Critical Infrastructure Sectors

28 October

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

This document is the result of a July 2021 security memorandum signed by President Biden. It has tasked CISA and the NIST with creating fundamental cybersecurity practices for critical infrastructure, mainly to help small- and medium-sized enterprises (SMEs) improve their cybersecurity efforts. The goals have been established based on existing cybersecurity frameworks and guidance. They also rely on real-world threats and adversary tactics, techniques, and procedures (TTP) observed by CISA and its partners. "By implementing these goals, owners and operators will reduce risks to critical infrastructure operations and the American people," the report reads. CISA plans to update these goals every six to 12 months.

REFERENCE:
CISA Issues report outlining baseline cybersecurity performance goals (CPGs) for all critical infrastructure sectors - Infosecurity Magazine

Data Breach of Missile Maker MBDA May Have Been Real: CloudSEK

31 October

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

In July, the Adrastea threat group announced a data breach from MBDA, a European missile manufacturer with ties to NATO. At the time, MBDA refuted the claims, saying that while some files were stolen, MBDA was not hacked, and its security systems remained intact. Further, the missile maker said the data made available online was "neither classified data nor sensitive."

Security researchers at CloudSEK have now written a new advisory about the alleged hacking campaign against MBDA. The technical write-up says CloudSEK's researchers were able to obtain and analyze the password-protected ZIP file containing the samples for the data breach. According to CloudSEK, the folder included files detailing confidential, personally identifiable information (PII) of MBDA's employees, alongside multiple standard operating procedures (SOPs) underlying the requirements for NATO's Counter Intelligence to avert threats related to Terrorism, Espionage, Sabotage, and Subversion (TESS).

REFERENCE:
Data Breach of Missile Maker MBDA May Have Been Real: CloudSEK - Infosecurity Magazine

SANS Survey: OT/ICS Cybersecurity Threats Remain High

31 October

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

The SANS 2022 operational technology/industrial control systems (OT/ICS) Cybersecurity Report, a SANS Institute survey sponsored by Nozomi Networks, shows some interesting trends in operational security. A few key points of the survey include:

- 62% of respondents rated the risk to their OT environment as high or severe.
- 39.7% of respondents said that Ransomware and financially motivated cybercrimes topped the list of threat vectors, followed by nation-state-sponsored attacks (38.8%). Non-ransomware criminal attacks came in third (cited by 32.1%), followed closely by hardware/software supply chain risks (30.4%).
- While the number of respondents who said they had experienced a breach in the last 12 months dropped to 10.5% (down from 15% in 2021), 35% of those said the engineering workstation was an initial infection vector (doubling from 18.4% last year).
- 66% say their control system security budget increased over the past two years (up from 47% last year).
- 56% say they are now detecting compromises within the first 24 hours of an incident (up from 51% in 2021).
- 69% say they move from detection to containment within 6 to 24 hours.
- 87.5% have conducted a security audit of their OT/control systems or networks in the past year (up from 75.9% last year) – one-third (29%) have now implemented a continual assessment program.
- 83% monitor their OT system security. Of those, 41% used a dedicated OT SOC.

REFERENCE:
Industrial providers ramp up cyber risk posture as OT threats evolve – Cybersecurity Dive

CISA Publishes Multi-Factor Authentication Guidelines to Tackle Phishing

31 October

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

The Cybersecurity and Infrastructure Security Agency (CISA) has published two fact sheets designed to highlight threats against accounts and systems using certain forms of multi-factor authentication (MFA). “CISA strongly urges all organizations to implement phishing-resistant MFA to protect against phishing and other known cyber-threats,” the Agency wrote, commenting on the news. The first of the two documents describes multiple methods threat actors have used to gain access to MFA credentials, including phishing, push bombing (AKA, push fatigue), exploitation of Signaling System No. 7 (SS7) protocol vulnerabilities, and SIM swap. The second fact sheet provides additional information about threats and defense against accounts and systems using mobile push notification-based MFA. It includes information on how MFA prompts work, how to mitigate threats targeting these systems, and best practices for using MFA with number matching. Dragos strongly recommends using MFA against phishing and other threats.

REFERENCE:
CISA MFA Fact Sheets – CISA
CISA Publishes Multi-Factor Authentication Guidelines to Tackle Phishing - Infosecurity Magazine

US Electric Cooperatives Awarded $15 Million to Expand ICS Security Capabilities

02 November

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

The US Department of Energy has awarded $15 million to the National Rural Electric Cooperative Association (NRECA) in an effort to help electric cooperatives expand their cybersecurity capabilities for industrial control systems (ICS). Specifically, electric cooperatives can use the funds to identify and deploy cyber monitoring technologies for ICS. The money will be awarded over a period of three years, with $10 million disbursed in 2022 and the remaining amount over the following years. NRECA represents nearly 900 local electric cooperatives in the United States, serving a combined 42 million Americans.

"As threats and threat actors evolve, electric cooperatives consistently work to improve their cyber defenses. Funding like this helps co-ops stay ahead of the curve," said NRECA CEO Jim Matheson. "Our longstanding partnership with DOE makes the electric grid more resilient, reliable, and secure.

REFERENCE:
US Electric Cooperatives Awarded $15 Million to Expand ICS Security Capabilities – SecurityWeek

New EU Cyber Security Rules for Airlines Impact Manufacturers/Supply Chain

02 November 3, 2022

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

New cybersecurity rules in Europe will for the first time require a swath of aviation suppliers to identify and defend against hacking risks to flight safety. The new rules, which take effect in 2025, will apply to a range of air transportation companies, including manufacturers, suppy chain partners, airlines, airports, flight training schools, caterers, and weather data providers. Companies also will be required to create a governance system that assigns an individual to be responsible for making sure problems are documented and addressed.

REFERENCE:
EU Expands Cyber Rules for Airline Flight Safety - Wall Street Journal

Ransomware Roundup

Ransomware attacks increasingly target and compromise industrial companies globally, often disrupting operations. This section provides a list of ransomware targeting industrial and related entities, overviews of known compromises, ransomware groups' activity, and defensive recommendations.

Ransomware Shifts Toward Destructive Attacks as 'Geopolitical Tensions' Take Hold

27 October

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

Dragos is tracking a shift in ransomware activity targeting critical infrastructure, with destructive attacks more common as geopolitical events like the Russia/Ukraine war and tensions between Albania and Iran take hold. Some ransomware groups are shifting focus from financial gains to destructive attacks under growing geopolitical tension and economic turbulence. The global energy crisis triggered by Russia's invasion of Ukraine may also lead to an increase in ransomware activities targeting the energy sector, according to Dragos. The Colonial Pipeline attack carried out by the Russian-based cybercriminal group DarkSide in 2021 has highlighted an urgent need for the US to defend the country's critical infrastructure from malicious actors. However, even as subsequent international government and law enforcement actions drove groups like DarkSide underground, new threat actors, such as Ragnar Locker, have become prevalent within the ransomware family. Dragos researchers warned that besides those new ransomware gangs that emerged in Q3, more groups would appear in the next quarter due to the leaking of the LockBit 3.0 builder.

"While it is quite easy to speculate about whether a new ransomware group has roots in or is reformed from another one, confidence levels surrounding such assessments require deep analysis of the code the ransomware groups use for TTPs such as initial access, credential harvesting, lateral movement, filesystem enumerations, and encryption. It is, therefore, too early for Dragos to determine similarities between groups beyond what is publicly reported," Tom Winston, director of intelligence content at Dragos, told SC Media.

The Dragos report indicates that the manufacturing sector remains the most targeted sector in critical infrastructure, with 68 percent of observed attacks, the same percentage reported in Q2. As for other industrial segments, nine percent of attacks targeted the food and beverage sector, followed by six percent targeting the oil and natural gas sector. The energy sector and pharmaceuticals sectors collectively account for 10 percent of attacks.

REFERENCE:
Ransomware shifts toward destructive attacks as 'geopolitical tensions' take hold – SC Magazine
Dragos Industrial Ransomware Analysis: Q3 2022 – Dragos, Inc.

LockBit Dominates Ransomware Campaigns in 2022: Deep Instinct

01 November

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

The LockBit Ransomware-as-a-Service (RaaS) group accounted for 44% of all ransomware campaigns overall in 2022, followed by Conti (23%), Hive (21%), Black Cat (7%), and Conti Splinters (5%), the latter group comprising threat actors from Quantum, BlackBast, and BlackByte. These figures come from the 2022 Interim Cyber Threat Report by Deep Instinct, which the company has shared with Infosecurity. "2022 has been another record year for cyber-criminals and ransomware gangs," commented Mark Vaitzman, threat lab team leader at Deep Instinct. "It's no secret that these threat actors are constantly upping their game with new and improved tactics designed to evade traditional cyber defenses."

REFERENCE:
LockBit Dominates Ransomware Campaigns in 2022: Deep Instinct – Infosecurity Magazine

Ransomware Families Post Industrial Firms on Dedicated Leak Sites

27 Oct – 2 Nov 2022

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

Dragos identified information about industrial firms on Dedicated Leak Sites (DLS) maintained by ransomware gangs from 27 Oct – 2 Nov 2022. The presence of this information does not guarantee a compromise and is for customer awareness only.

- Lockbit 3.0 posted information regarding two metal products manufacturing entities in the U.S., an aerospace manufacturing entity in France, a pharmaceuticals entity in Uruguay, an elevator manufacturing entity in Italy, and a tools manufacturing entity in the U.S.
- Karakurt posted information regarding two pharmaceuticals entities in the U.K, a metal products manufacturing entity in Turkey, and an Oil and Gas entity in Vietnam.
- Black Basta posted information regarding a lightning manufacturing entity and an aerospace manufacturing entity in the U.S.
- AlphaV posted information regarding a furniture manufacturing entity in China.
- LV posted information regarding a power supplies manufacturing entity in Switzerland
- Mollox posted information regarding an automotive manufacturing entity in Malaysia and a machinery manufacturing entity in Canada.
- Ragnar Locker posted information regarding a building supplies manufacturing entity in the U.S.
- Vice Society posted information regarding a metal products manufacturing entity in the U.S.,

Recommendations:

- Ensure employees are trained to recognize phishing campaigns and report them to security personnel.
- Implement flagging or other methods to tag external emails 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.
- Patch corporate networks thoroughly to prevent malware infections targeting disclosed vulnerabilities entering the environment and 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 IT and 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.
- Enable and test Data Loss Prevention (DLP) Technologies and monitor anomalous outbound data flow.

Vulnerability Advisories

11 This week, an independent Dragos analysis identified eleven individual vulnerabilities (CVE) with incorrect data out of 37 total - a 30% error rate. Nine of the eleven were found to be more severe and two of the eleven were found to be less severe. The corrected data are included in the advisories below.

Trihedral VTScada

27-October-2022

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

Trihedral's VTScada is a Supervisory Control and Data Acquisitions (SCADA) software, deployed worldwide and commonly seen in the energy, water, and wastewater industries.

Key Takeaways:

- There is a vulnerability in Trihedral's VTScada that could allow an adversary to deny availability.
- An unauthenticated and remote adversary could cause a Denial of Service (DoS) condition through maliciously crafted HTTP requests.
- Restrict access to HTTP (TCP/80) and HTTPS (TCP/443).

Trihedral VTScada	**Attributes**		**Description**
Date: Oct 27, 2022 Source: ICS-CERT CVE-2022-3181	Public Proof of Concept Exists Active Exploitation Skill Level Required	No No Low	Successful exploitation could allow an unauthenticated and remote adversary to cause a DoS condition through maliciously crafted HTTP requests.
Dragos Assessment Restrict access to HTTP (TCP/80) and HTTPS (TCP/443).	**Access Level Required** Remotely Exploitable Physical Access Required Known Credentials User Interaction	 ✓	**Affecting** • VTScada v12.0.38 and prior.
	Security Impact		

Patch/Defense Details Update to a patched version, v12.0.39 or later.	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 ✓	**Additional Resources** ICSA-22-300-04

SAUTER Controls moduWeb

27-October-2022

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

SAUTER Controls moduWeb is used to monitor building and control networks and devices, deployed worldwide and commonly seen in the critical manufacturing and energy industry.

Key Takeaways:

- There is a vulnerability in SAUTER Controls moduWeb that could allow an adversary to disclose information and execute code.
- An unauthenticated and remote adversary could obtain sensitive information and execute malicious HTML/JS code by tricking an authenticated user into clicking a crafted link.
- Restrict access to HTTP (TCP/80) and HTTPS (TCP/443). Train users to only click links from trusted sources.

Note:
CVE-2022-40190 appears to have an incorrect CVSS. Dragos assesses that the score should be:
8.8 => **9.6**
AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H => AV:N/AC:L/PR:N/UI:R/***S:C***/C:H/I:H/A:H

SAUTER Controls moduWeb

Date: Oct 27, 2022
Source: ICS-CERT
CVE-2022-40190

Dragos Assessment 
Restrict access to HTTP (TCP/80) and HTTPS (TCP/443). Train users to only click links from trusted sources.

Patch/Defense Details
Update to a patched version, v3.1.3 or later.

Attributes	
Public Proof of Concept Exists	No
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 to obtain sensitive information and execute malicious HTML/JS code by tricking an authenticated user into clicking a crafted link.

Affecting

- SAUTER moduWeb: v2.7.1

Additional Resources
ICSA-22-300-02

Rockwell Automation FactoryTalk Alarm and Events Server

27-October-2022

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

Rockwell FactoryTalk Alarms and Events is the notifications platform used by most Rockwell Automation software. They are deployed worldwide and commonly seen in the chemical, critical manufacturing, food and agriculture, water and wastewater systems.

Key Takeaways:

- There is a vulnerability in Rockwell Automation FactoryTalk Alarm and Events Server that could allow an adversary to deny availability.
- An unauthenticated and remote adversary that can open a connection to vulnerable devices could cause a Denial of Service (DoS) condition through crafted packets.
- Restrict access to FactoryTalk Alarming Server (TCP/6543) and Event Server (TCP/7700). Ensure the host systems are segmented from the Enterprise network and the internet.

Rockwell Automation FactoryTalk Alarm and Events Server

Date: Oct 27, 2022
Source: ICS-CERT
CVE-2022-38744

Dragos Assessment 
Restrict access to FactoryTalk Alarming Server (TCP/6543) and Event Server (TCP/7700).

Patch/Defense Details
Rockwell Automation has not resleased a patch to resolve this issue.

Attributes	
Public Proof of Concept Exists	No
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 that manages to open a connection to vulnerable devices to cause a DoS condition through crafted packets.

Affecting

- FactoryTalk Alarm and Events Server: All versions.

Additional Resources
Rockwell Automation Security Advisory: PN1605
ICSA-22-300-01

Rockwell Automation Stratix Devices Containing Cisco IOS

27-October-2022

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

Rockwell Automation Stratix devices are industrial ethernet switches, deployed worldwide and seen across a variety of industries.

Key Takeaways:

- There are multiple vulnerabilities in Rockwell Automation Stratix devices containing Cisco IOS XE and Cisco IOS software that could allow an adversary to deny availability and execute code.
- An authenticated and remote adversary could execute code with either administrative or root privileges through malicious requests, user inputs, and malicious file uploads. An adversary could also leverage the vulnerabilities to restart the device, resulting in a Denial of Service (DoS), write and view files on the operating system or host device through malicious pathnames,ands upload malicious images during the boot process.
- Restrict access to HTTP (TCP/80), HTTPS (TCP/443), and SSH (TCP/22). Monitor logs for suspicious authentication attempts and requests containing traversal characters such as "../".

Note:
CVE-2020-3229 appears to have an incorrect CVSS. Dragos assesses that the score should be:
8.8 => **9.9**
AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H => AV:N/AC:L/PR:L/UI:N/***S:C***/C:H/I:H/A:H
CVE-2020-3219 appears to have an incorrect CVSS. Dragos assesses that the score should be:
8.8 => **9.9**
AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H => AV:N/AC:L/PR:L/UI:N/***S:C***/C:H/I:H/A:H
CVE-2020-3211 appears to have an incorrect CVSS. Dragos assesses that the score should be:
7.2 => **9.1**
AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H => AV:N/AC:L/PR:H/UI:N/***S:C***/C:H/I:H/A:H
CVE-2020-3218 appears to have an incorrect CVSS. Dragos assesses that the score should be:
7.2 => **9.1**
AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H => AV:N/AC:L/PR:H/UI:N/***S:C***/C:H/I:H/A:H
CVE-2020-3209 appears to have an incorrect CVSS. Dragos assesses that the score should be:
6.8 => **7.6**
AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H => AV:P/AC:L/PR:N/UI:N/***S:C***/C:H/I:H/A:H
CVE-2021-1385 appears to have an incorrect CVSS. Dragos assesses that the score should be:
6.5 => **7.2**
AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N => AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/***A:H***
CVE-2020-3516 appears to have an incorrect CVSS. Dragos assesses that the score should be:
4.3 => **6.5**
AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L => AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/***A:H***

Rockwell Automation Stratix Devices Containing Cisco IOS Date: Oct 27, 2022 Source: ICS-CERT CVE-2020-3229 CVE-2020-3219	**Attributes**		**Description**
	Public Proof of Concept Exists	No	Successful exploitation could allow an authenticated and remote adversary to execute code with either administrative or root privileges through malicious requests, user inputs, and malicious file uploads. An
	Active Exploitation	No	
	Skill Level Required	Low	
	Access Level Required		
	Remotely Exploitable	✓	

<table>
<tr>
<td>CVE-2021-1446
CVE-2020-3200
CVE-2020-3211
CVE-2020-3218
CVE-2020-3209
CVE-2021-1385
CVE-2020-3516

Dragos Assessment
Restrict access to HTTP (TCP/80), HTTPS (TCP/443), and SSH (TCP/22). Monitor logs for suspicious authentication attempts and requests containing traversal characters such as "../".

Patch/Defense Details
Update to a patched version:
Stratix 5800 switches (All listed vulnerabilities except CVE-2020-3200): Stratix 5800 v17.04.01 or later
Stratix 5800 switches (CVE-2020-3200): v16.12.01 or later
Stratix 5400/5410 switches (CVE-2020-3200 only): v15.2(7)E2 or later</td>
<td>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 ✓</td>
<td>adversary could also leverage the vulnerabilities to restart the device, resulting in a DoS, write and view files on the operating system or host device through malicious pathnames, and upload malicious images during the boot process.

Affecting
The following Rockwell Automations products contain Cisco IOS XE and Cisco IOS software:
• Stratix 5800 switches: Prior to v16.12.01
• Stratix 5400 switches: Prior to v15.2(7)E2 (CVE-2020-3200 only)
• Stratix 5410 switches: Prior to v15.2(7)E2 (CVE-2020-3200 only)

Additional Resources
Rockwell Automation's Recommended Security Guide
ICSA-22-300-03</td>
</tr>
</table>

Delta Electronics InfraSuite Device Master

25-October-2022

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

Delta Electronics InfraSuite Device Master is a real-time device monitoring software, deployed worldwide and commonly seen in the energy industry.

Key Takeaways:

- There are multiple vulnerabilities in Delta Electronics InfraSuite Device Master that could allow an adversary to carry out functions, escalate privileges, deny availability, and execute code.
- An unauthenticated and remote adversary could execute code and create users with admin privileges through malicious serialized objects, execute code through malicious Zip files, and by tricking a user into connecting to a malicious server. An authenticated and remote adversary could also leverage the vulnerable authentication mechanism to cause a Denial of Service (DoS), change user group privileges, escalate privileges, and modify the UserListInfo.xml configuration file to view or change administrative passwords.
- Restrict access to HTTP (TCP/80) and HTTPS (TCP/443). Train users to only load trusted files into the application, especially of type *.zip. Monitor logs for suspicious authentication attempts and requests containing traversal characters such as "../".

Delta Electronics InfraSuite Device Master

Date: Oct 25, 2022
Source: ICS-CERT
CVE-2022-41778
CVE-2022-38142
CVE-2022-41779
CVE-2022-41657
CVE-2022-41772
CVE-2022-40202
CVE-2022-41688
CVE-2022-41644
CVE-2022-41776
CVE-2022-41629

Dragos Assessment

Restrict access to HTTP (TCP/80) and HTTPS (TCP/443). Train users to only load trusted files into the application, especially of type *.zip. Monitor logs for suspicious authentication attempts and requests containing traversal characters such as "../".

Attributes	
Public Proof of Concept Exists	No
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 to execute code and create users with admin privileges through malicious serialized objects and execute code through malicious *.zip files, and trick a user into connecting to a malicious server. An authenticated and remote adversary could also leverage the vulnerable authentication mechanism to cause a DoS, change user group privileges, escalate privileges, and modify the UserListInfo.xml configuration file to view or change administrative passwords.

Affecting

- InfraSuite Device Master: v00.00.01a and prior.

Patch/Defense Details Update to a patched version, v00.00.02a, or later. Delta recommends that users install the new version through the official installer.		**Additional Resources** ICSA-22-298-07

Johnson Controls CKS CEVAS

25-October-2022

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

CKS CEVAS is a web-based billing and reporting solution, deployed worldwide and commonly seen in the critical manufacturing industry.

Key Takeaways:

- There is a vulnerability in Johnson Controls CKS CEVAS that could allow an adversary to obtain data.
- An unauthenticated and remote adversary could obtain data through crafted SQL queries.
- Restrict access to the web server, typically found on HTTP (TCP/80), and HTTPS (TCP/443). Ensure host systems are segmented from the Enterprise network and the internet.

Note:
CKS is a subsidiary of Johnson Controls Inc.
CVE-2021-36206 appears to have an incorrect CVSS. Dragos assesses that the score should be:
10 => **7.5**
AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N => AV:N/AC:L/PR:N/UI:N/***S:U***/C:H/***I:N***/A:N

Johnson Controls CKS CEVAS

Date: Oct 25, 2022
Source: ICS-CERT
CVE-2021-36206

Dragos Assessment 
Restrict access to the web server, typically found on HTTP (TCP/80), and HTTPS (TCP/443). Ensure host systems are segmented from the Enterprise network and the internet.

Patch/Defense Details
Contact Johnson CKS to update to a patched version, v1.01.46 or later.

Attributes	
Public Proof of Concept Exists	No
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 to obtain data through crafted SQL queries.

Affecting

- CKS CEVAS: Prior to v1.01.46

Additional Resources
Johnson Controls Advisory: JCI-PSA-2022-15
ICSA-22-298-05

Siemens Siveillance Video Mobile Server

25-October-2022

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

Siemens Siveillance Video is an IP video management software, deployed worldwide and commonly seen in the commercial facilities and communications industry.

Key Takeaways:

- There is a vulnerability in Siemens Siveillance Video that could allow an adversary to gain unauthorized access.
- An unauthenticated and remote adversary could leverage the vulnerable authentication mechanism to gain unauthorized access to the application.
- Enable the feature Servers > Mobile Servers > Deny the built-in Administrators role access to the mobile servers for all configured mobile servers.

Note:
Siemens Siveillance Video was formerly called Siveillance VMS.

Siemens Siveillance Video Mobile Server

Date: Oct 25, 2022
Source: ICS-CERT
CVE-2022-43400

Dragos Assessment 
Enable the feature Servers > Mobile Servers > Deny the built-in Administrators role access to the mobile servers for all configured mobile servers.

Patch/Defense Details
Update to a patched version, v22.2a(80) or later.

Attributes	
Public Proof of Concept Exists	No
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 that leverages the vulnerable authentication mechanism to gain unauthorized access to the application.

Affecting

- Siemens Siveillance Video: Prior to v22.2a(80)

Additional Resources
Siemens Security Advisory: SSA-640732
ICSA-22-298-03

HEIDENHAIN Controller TNC on HARTFORD Machine

25-October-2022

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

HEIDENDAIN Controller TNC is a computer numerical control (CNC) controller, deployed worldwide and seen across a variety of industries.

Key Takeaways:

- There is a vulnerability in HEIDENHAIN Controller that could allow an adversary to gain unauthorized access.
- An unauthenticated and remote adversary could leverage the vulnerable authentication mechanism to gain unauthorized access to the device.
- Restrict access to LSV2 (TCP/19000) and block DNC communication through the controllers HEROS operating system.

Note:
CVE-2022-41648 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

HEIDENHAIN Controller TNC on HARTFORD Machine

Date: Oct 25, 2022
Source: ICS-CERT
CVE-2022-41648

Dragos Assessment
Restrict access to LSV2 (TCP/19000) and block DNC communication through the controllers HEROS operating system.

Patch/Defense Details
HEIDENDAIN has not released a patch to resolve this issue.

Attributes	
Public Proof of Concept Exists	No
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 that leverages the vulnerable authentication mechanism to gain unauthorized access to the device.

Affecting

- HEIDENHAIN Controller TNC 640: v340590 07 SP5 Running HEROS v5.08.3 controlling HARTFORD 5A-65E CNC machine.

Additional Resources
ICSA-22-298-02

Haas Controller

25-October-2022


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

Haas Automation's Haas Controller is a Computer Numerical Control (CNC), deployed worldwide and commonly seen in the critical manufacturing industry.

Key Takeaways:

- There are multiple vulnerabilities in Haas Automation's Haas Controller that could allow an adversary to carry out functions and disclose information.
- An unauthenticated and remote adversary could leverage the Ethernet Q Commands service to write malicious macros to the vulnerable device. An adversary could also capture network traffic between the controller to view sensitive information.
- Enable authentication for the Ethernet Q Commands service. Ensure there is a set limit of macros that can be written. Ensure host systems are segmented from the Enterprise network and the internet.

Note:
CVE-2022-41636 appears to have an incorrect CVSS. Dragos assesses that the score should be:
9.1 => **7.5**
AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N => AV:N/AC:L/PR:N/UI:N/S:U/C:H/***I:N***/A:N

Haas Controller

Date: Oct 25, 2022
Source: ICS-CERT
CVE-2022-2474
CVE-2022-2475
CVE-2022-41636

Dragos Assessment 
Enable authentication for the Ethernet Q Commands service. Ensure there is a set limit of macros that can be written. Ensure host systems are segmented from the Enterprise network and the internet.

Patch/Defense Details
Haas Automation has not released a patch to resolve these issues.

Attributes	
Public Proof of Concept Exists	No
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 that leverages the Ethernet Q Commands service to write malicious macros to the vulnerable device. An adversary could also capture network traffic between the controller to view sensitive information.

Affecting

- Haas Controller: v100.20.000.1110

Additional Resources
ICSA-22-298-01

Delta Electronics DIAEnergie

25-October-2022

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

Delta Electronics' DIAEnergie is an Energy Management System (EMS) deployed worldwide and commonly seen in the critical manufacturing industry.

Key Takeaways:

- There is a vulnerability in Delta Electronics DIAEnergie that could allow an adversary to execute code.
- An authenticated and remote adversary could inject malicious code on vulnerable pages, resulting in code execution when an authenticated user visits the vulnerable page as well as execute malicious SQL queries against the application database through vulnerable parameters.
- Restrict access to HTTP (TCP/80) and HTTPS (TCP/443). Monitor logs for suspicious or unfamiliar login attempts.

Delta Electronics DIAEnergie

Date: Oct 25, 2022
Source: ICS-CERT
CVE-2022-41701
CVE-2022-40965
CVE-2022-41555
CVE-2022-41702
CVE-2022-41651
CVE-2022-41133
CVE-2022-41773

Dragos Assessment 

Restrict access to HTTP (TCP/80) and HTTPS (TCP/443). Monitor logs for suspicious or unfamiliar login attempts.

Patch/Defense Details

Update to a patched version, v1.9.01.002 or later.

Attributes	
Public Proof of Concept Exists	No
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 authenticated and remote adversary to inject malicious code on vulnerable pages, resulting in code execution when an authenticated user visits the vulnerable page as well as execute malicious SQL queries against the application database through vulnerable parameters.

Affecting

- DIAEnergie: Prior to v1.9.01.002

Additional Resources

ICSA-22-298-06

Hitachi Energy MicroSCADA X DMS600

25-October-2022

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

Hitachi Energy MicroSCADA X DMS600 is a Distribution Management System (DMS), deployed worldwide and commonly seen in the energy industry.

Key Takeaways:

- There are multiple vulnerabilities in Hitachi Energy MicroSCADA X DMS600 that could allow an adversary to disclose and modify data.
- An authenticated and local adversary with access to PostgreSQL could disclose sensitive information and overwrite data through maliciously crafted SQL commands.
- Restrict access to PostgreSQL (TCP/5432). Monitor logs for suspicious or unfamiliar login attempts.

Note:
Although these vulnerabilities are remotely exploitable in other Hitachi Energy products, remote access to DMS600 is not possible by default.

Hitachi Energy MicroSCADA X DMS600

Date: Oct 25, 2022
Source: ICS-CERT
CVE-2021-32027
CVE-2021-32028

Dragos Assessment
Restrict access to PostgreSQL (TCP/5432). Monitor logs for suspicious or unfamiliar login attempts.

Patch/Defense Details
Update to a patched version, v4.6 or later.

Attributes	
Public Proof of Concept Exists	No
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 authenticated and remote adversary with access to PostgreSQL to disclose sensitive information and overwrite data through maliciously crafted SQL commands.

Affecting

- DMS600: v4.5

Additional Resources
Hitachi Energy's Security Advisory. ICSA-22-298-04