



## Executive Summary

- Microsoft fixes Exchange server zero-day
- Zoho password manager torched by Godzilla webshell
- Sunwater unaware of cyber-attack for nine months
- Babuk ransomware seen exploiting ProxyShell vulnerabilities
- Healthcare & OT systems exposed to attacks
- Two NPM packages with 22 million weekly downloads found backdoored
- Critical flaws in Philips TASY EMR could expose patient data
- Multiple BusyBox security bugs threaten embedded Linux devices
- 14 new vulnerabilities discovered in BusyBox
- New Android spyware poses Pegasus-Like threat
- Palo Alto warns of Zero-Day bug in firewalls using GlobalProtect portal VPN
- Citrix application delivery controller, Citrix gateway, and Citrix SD-WAN WANOP edition appliance security update
- Nearly 100 TCP/IP stack vulnerabilities found during 18-month research project

**General vulnerabilities:** Microsoft Excel, SAP, Adobe, Citrix, Samba, Microsoft, Apple, VMware

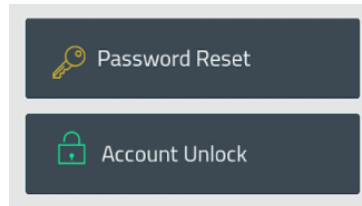
**IoT, OT & ICS vulnerabilities:** Philips, Schneider Electric NMC, Schneider Electric GUIcon, Siemens Nucleus net, mySCADA, OSIsoft, OSIsoft PI Web API, Advantech, Siemens SIMATIC WinCC, Siemens Mendix, Siemens Mendix Studio Pro, Siemens SCALANCE W1750D, Siemens Nucleus RTOS-based APOGEE and TALON Products, Siemens NX OBJ Translator, Siemens Climatix POL909, Siemens SENTRON powermanager, WECON PLC Editor, Multiple Data Distribution Service (DDS) Implementations

## News This Week...

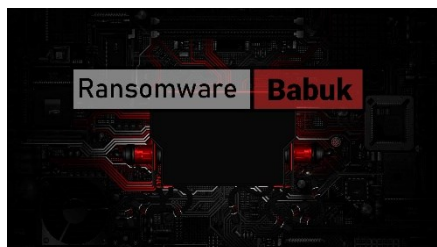


**Microsoft's November security updates** contained fixes for fifty-five vulnerabilities, including six zero-day flaws. The flaw organizations should be most concerned about is CVE-2021-42298, a critical bug in Microsoft Defender that an attacker can exploit to remotely execute malicious code on vulnerable systems. Microsoft has self-assessed the flaw as severe.

A new campaign is prying apart a known security vulnerability in the **Zoho ManageEngine ADSelfService Plus Password Manager**. The threat actors have managed to exploit the Zoho weakness in at least nine global entities across multiple critical sectors (technology, defence, healthcare, energy, and education), deploying the Godzilla webshell and exfiltrating data. The bug is a critical authentication bypass flaw – CVE-2021-40539 – that allows unauthenticated remote code execution (RCE). The consequences of a successful exploit can be significant.



Queensland's largest regional water supplier was targeted by hackers in a cyber security breach that went undetected for nine months, leaving suspicious files on a webserver to redirect visitor traffic to an online video platform. **Sunwater** has admitted the cyber breach after the tabling of a Queensland's Audit Office report into the state's water authorities. No financial or customer data is believed to have been leaked and immediate steps have been to improve security once the unauthorized access to an online content management system was detected.



A newly observed **Babuk ransomware** campaign is targeting ProxyShell vulnerabilities in Microsoft Exchange Server. Researchers spotted signs that the attackers are leveraging a China Chopper webshell for the initial compromise, and then use that for the deployment of Babuk. Tracked as CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207, the issues were addressed in April and May, with technical details made public in August. Researchers say that the Tortilla threat actor, active since July 2021, has started targeting the Exchange Server flaws. The infection chain features an intermediate unpacking module that is downloaded from pastebin.pl (a pastebin.com clone) and then decoded in memory before the final payload is decrypted and executed.

A series of thirteen vulnerabilities identified in the **Nucleus TCP/IP stack** could be exploited to execute code remotely, cause a denial-of-service condition, or to obtain sensitive information. The issues affect safety-critical devices, such as anesthesia machines, patient monitors and other types of devices used in healthcare. Other types of operational technology (OT) systems are also impacted. The most important of the newly identified issues is CVE-2021-31886, a stack-based buffer overflow that exists because the FTP server fails to properly validate the length of the "USER" command. An attacker could exploit the vulnerability to cause a denial-of-service (DoS) condition or to achieve remote code execution. Two other similar issues in the FTP server were assessed with a severity rating of high. Of the remaining bugs, nine are considered high severity and could be exploited to leak sensitive information or cause DoS conditions. The last issue in the set is a medium-severity bug in the ICMP that could be exploited to send ICMP echo reply to messages to arbitrary network systems.



Two popular **NPM** packages with cumulative weekly downloads of twenty-two million were found to be compromised with malicious code by gaining unauthorized access to the respective developer's accounts. The two libraries in question are 'coa', a parser for command-line options, and 'rc', a configuration loader, both of which were tampered with by an unidentified threat actor to include identical password-stealing malware. All versions of 'coa' starting with 2.0.3 and above are impacted, and users of the affected versions are advised to downgrade to 2.0.2 as soon as possible and check their systems for suspicious activity. Similarly, versions 1.2.9, 1.3.9, and 2.3.9 of 'rc' have been found laced with malware, with an independent alert urging users to downgrade to version 1.2.8. To protect your accounts and packages from similar attacks, it is highly recommend enabling multi-factor authentication on your NPM account.

Critical vulnerabilities affecting **Philips Tasy Electronic Medical Records (EMR)** system could be exploited by remote threat actors to extract sensitive personal data from patient databases. Successful exploitation of these vulnerabilities could result in patients' confidential data being exposed or extracted from Tasy's database, give unauthorized access, or create a denial-of-service condition. Used by multiple healthcare institutions, Philips Tasy EMR is designed as an integrated healthcare informatics solution that enables centralized management of clinical, organizational, and administrative processes, including incorporating analytics, billing, and inventory and supply management for medical prescriptions. All healthcare providers using a vulnerable version of the EMR system are recommended to update to version 3.06.1804 or later as soon as possible to prevent potential real-world exploitation.



Researchers have discovered 14 critical vulnerabilities in a popular program used in embedded Linux applications, all of which allow for denial of service (DoS) and 10 enabling remote code execution. One of the flaws also may allow devices to leak info. The two firms teamed up to take a deeper dive into **BusyBox**, a software suite used by many of the world's leading operational technology (OT) and internet of things (IoT) devices. The discovery of the flaws is significant because of the proliferation of BusyBox not just for the embedded Linux world, but also for numerous Linux applications outside of devices. These new vulnerabilities disclosed only


Researchers have discovered a new Android spyware that provides similar capabilities to NSO Group's Pegasus controversial software. Called **PhoneSpy**, the mobile surveillance-ware has been spotted actively targeting South Koreans without their knowledge. It disguises itself as a legitimate application and gives attackers complete access to data stored on a mobile device, granting full control over the targeted device. The spyware, potentially more dangerous than Pegasus, hides in plain sight, disguising itself as a regular application with purposes ranging from learning yoga to watching TV and videos, or browsing photos. PhoneSpy features include stealing data, eavesdropping on messages, and viewing images stored on the phone. Attackers can also gain full remote control of Android phones with it so far identified within twenty-three applications.




**Palo Alto Networks** have released security advisories affecting multiple versions of PAN-OS. This includes a critical zero day, tracked as [CVE 2021-3064](#) and scoring a CVSS rating of 9.8 out of 10 for vulnerability severity, is in PAN's [GlobalProtect firewall](#). It allows for unauthenticated RCE on multiple versions of PAN-OS 8.1 prior to 8.1.17, on both physical and virtual firewalls. We encourage administrators to visit PAN's [security advisory](#) page for more information.



## Industrial Control Systems (ICS) & IoT Vulnerabilities...

<b>CVSS v3:</b>	<b>6.2</b>	
<b>Attention:</b>	Low attack complexity	
<b>Vendor:</b>	<b>Philips</b>	
<b>Equipment:</b>	<b>MRI 1.5T and 3T</b>	
<b>Vulnerabilities:</b>	Improper Access Control, Incorrect Ownership Assignment, Exposure of Sensitive Information to an Unauthorised Actor	
<b>Risk Evaluation:</b>	Successful exploitation of these vulnerabilities may allow an unauthorized attacker access to execute software, modify system configuration, view/update files, and export data (including patient data) to an untrusted environment.	
<b>Affected Versions:</b>	Philips reports the vulnerabilities affect the following MRI products:	
	<ul style="list-style-type: none"> <li>• MRI 1.5T: Version 5.x.x</li> <li>• MRI 3T: Version 5.x.x</li> </ul>	
<b>Sectors:</b>	Healthcare and Public Health	
<b>Mitigation:</b>	Philips plans a new release to remediate these vulnerabilities by October 2022.	
	As an interim mitigation of these vulnerabilities, Philips recommends the following:	
	<ul style="list-style-type: none"> <li>• Users should operate all Philips deployed and supported products within Philips authorised specifications, including physical and logical controls. Only allowed personnel are permitted in the vicinity of the product. Refer to the Philips instructions for use (IFU) available on <a href="#">InCenter</a>.</li> </ul>	
	Users with questions about their specific MRI product should contact a Philips service support team or regional service support. Philips contact information is available at the <a href="#">Philips's customer service solutions website</a> .	

<b>CVSS v3:</b>	<b>6.8</b>	
<b>Attention:</b>	Exploitable remotely/low attack complexity	
<b>Vendor:</b>	<b>Schneider Electric</b>	
<b>Equipment:</b>	<b>Network Management Cards (NMC) and NMC Embedded Devices</b>	
<b>Vulnerabilities:</b>	Cross-site Scripting, Exposure of Sensitive Information to an Unauthorised Actor	
<b>Risk Evaluation:</b>	Successful exploitation of these vulnerabilities may allow data disclosure or cross-site scripting, which could result in an execution of malicious web code or a loss of device functionality.	
<b>Affected Versions:</b>	The following products are affected: Uninterruptible Power Supply (UPS) Products:	



- 1-Phase Uninterruptible Power Supply (UPS) using NMC2, including Smart-UPS, Symmetra, and Galaxy 3500 with Network Management Card 2 (NMC2): NMC2 AOS v6.9.8 and prior
- 3-Phase Uninterruptible Power Supply (UPS) using NMC2, including Symmetra PX 250/500 (SYPX) Network Management Card 2 (NMC2): NMC2 AOS v6.9.6 and prior
- 3-Phase Uninterruptible Power Supply (UPS) using NMC2 including Symmetra PX 48/96/100/160 kW UPS (PX2), Symmetra PX 20/40 kW UPS (SY3P), Gutor (SXW, GVX), and Galaxy (GVMTS, GVMSA, GVXTS, GVXSA, G7K, GFC, G9KCHU): NMC2 AOS v6.9.6 and prior
- 1-Phase Uninterruptible Power Supply (UPS) using NMC3 including Smart-UPS, Symmetra, and Galaxy 3500 with Network Management Card 3 (NMC3): NMC3 AOS v1.4.2.1 and prior

APC Power Distribution Products:

- APC Rack Power Distribution Units (PDU) using NMC2: NMC2 AOS v6.9.6 and prior
- APC Rack Power Distribution Units (PDU) using NMC3: NMC3 AOS v1.4.0 and prior
- APC 3-Phase Power Distribution Products using NMC2: NMC2 AOS v6.9.6 and prior
- Network Management Card 2 (NMC2) for InfraStruxure 150 kVA PDU with 84 Poles (X84P): NMC2 AOS v6.9.6 and prior
- Network Management Card 2 for InfraStruxure 40/60kVA PDU (XPDU): NMC2 AOS v6.9.6 and prior
- Network Management Card 2 for Modular 150/175kVA PDU (XRDP): NMC2 AOS v6.9.6 and prior
- Network Management Card 2 for 400 and 500 kVA (PMM): NMC2 AOS v6.9.6 and prior
- Network Management Card 2 for Modular PDU (XRDP2G): NMC2 AOS v6.9.6 and prior
- Rack Automatic Transfer Switches (ATS): NMC2 AOS v6.9.6 and prior

Environmental Monitoring:

- Environmental Monitoring Unit with embedded NMC2 (NB250) NetBotz NBRK0250: NMC2 AOS v6.9.6 and prior

Cooling Products:

- Network Management Card 2 (NMC2) Cooling Products: NMC2 AOS v6.9.6 and prior

Battery Management Products:

- Network Management Card 2 (NMC2) AP9922 Battery Management System (BM4): NMC2 AOS v6.9.6 and prior

**Sectors:**

**Mitigation:**

Energy

Schneider Electric recommends the following:

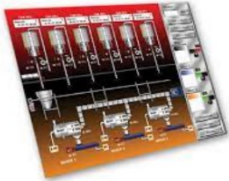


- 1-Phase Uninterruptible Power Supply (UPS) using NMC2: Update to v7.04 or later. SUMX and SY applications includes fixes for these vulnerabilities:
  - [SUMX \(SmartUPS & Galaxy 3500\)](#)
  - [SY \(Single Phase Symmetra\)](#)
  - [SUMX & SY Release notes](#)
- 3-Phase Uninterruptible Power Supply (UPS) using NMC2 including Symmetra PX 250/500 (SYPX) Network Management Card 2 (NMC2) (See [SEVD-2021-313-03](#) on what specific models are mitigated):
  - Update to v7.0.4 or later of the NMC2 SYPX application. Contact a [Schneider Electric support team](#) for SYPX application upgrade.
- 1-Phase Uninterruptible Power Supply (UPS) using NMC3: Update to v1.5 or later of the NMC3 SU and SY applications:
  - [SUMX \(SmartUPS & Galaxy 3500\)](#)
  - [SY \(Single Phase Symmetra\)](#)
  - [Release notes](#)
- APC Rack Power Distribution Units (PDU) using NMC2: Update to v7.0.6 or later of the NMC2 RPDU2G application:
  - [RPDU2G](#) (direct download)
- APC 3-Phase Power Distribution Products using NMC2: Update to v7.0.4 or later of the NMC2 RPP application:
  - [Galaxy RPP](#)
- Network Management Card 2 (NMC2) Cooling Products (See [SEVD-2021-313-03](#) on what specific series are mitigated): Update to v7.0.4 or later of the NMC2 of the cooling applications. Contact a [Schneider Electric support team](#) for upgrades.

For the products not listed above, Schneider Electric is in the process of establishing a remediation plan for affected NMC2 and NMC3 offers. This plan will include fixes or mitigations for these vulnerabilities. This document will be updated as remediations become available. Until then, users should immediately apply the following mitigations to reduce the risk of exploitation:



- NMC users should not trust links provided from sources that have not been verified as authentic.
- Ensure the workstation where the browser is being used is secured.
- If a debug.tar file is generated via Web or CLI, ensure it is deleted after retrieval.



<b>CVSS v3:</b>	<b>7.8</b>	
<b>Attention:</b>	Low attack complexity	
<b>Vendor:</b>	<b>Schneider Electric</b>	
<b>Equipment:</b>	<b>GUIcon</b>	
<b>Vulnerabilities:</b>	Out-of-bounds Write, Use After Free, Out-of-bounds Read	
<b>Risk Evaluation:</b>	Successful exploitation of these vulnerabilities may allow an attacker to execute arbitrary code on the host PC, leading to sensitive information disclosure or unintended user actions.	
<b>Affected Versions:</b>	The following versions of GUIcon software are affected: <ul style="list-style-type: none"><li>• GUIcon: Versions 2.0 (Build 683.003) and prior</li></ul>	
<b>Sectors:</b>	Critical Manufacturing	
<b>Mitigation:</b>	The GUIcon software tool was discontinued in June 2020 and is no longer supported. Users should immediately apply the following mitigation to reduce the risk of exploitation: <ul style="list-style-type: none"><li>• The only known method for an attacker to exploit these vulnerabilities is to create a malicious GUIcon *.gd1 configuration file and then trick a user into opening it with the GUIcon software. The mitigation for these vulnerabilities is to ensure any GUIcon *.gd1 file loaded into the tool is from a trusted source.</li><li>• For more information about these issues, please refer to the original Schneider Electric publication <a href="#">SEVD-2021-313-07</a></li></ul> Schneider Electric strongly recommends the following industry cybersecurity best practices: <ul style="list-style-type: none"><li>• Locate control and safety system networks and remote devices behind firewalls and isolate them from the business network.</li><li>• Install physical controls to prevent unauthorized personnel from accessing industrial control and safety systems, components, peripheral equipment, and networks.</li><li>• Place all controllers in locked cabinets and never leave them in the “Program” mode.</li><li>• Never connect programming software to any network other than the network intended for that device.</li><li>• Scan all methods of mobile data exchange with the isolated network, such as CDs, USB drives, etc., before use in the terminals or any node connected to these networks.</li><li>• Never allow mobile devices that have connected to any other network besides the intended network to connect to the safety or control networks without proper sanitation.</li><li>• Minimize network exposure for all control system devices and systems and ensure they are not accessible from the Internet.</li><li>• When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Recognize that VPNs may have vulnerabilities and should be updated to the most current</li></ul>	




version available. Also, understand that VPNs are only as secure as the connected devices.

<p><b>CVSS v3:</b></p> <p><b>Attention:</b></p> <p><b>Vendor:</b></p> <p><b>Equipment:</b></p> <p><b>Vulnerabilities:</b></p> <p><b>Risk Evaluation:</b></p> <p><b>Affected Versions:</b></p> <p><b>Sectors:</b></p> <p><b>Mitigation:</b></p>	<p><b>9.8</b></p> <p>Exploitable remotely/low attack complexity</p> <p><b>Siemens</b></p> <p><b>Nucleus Net, Nucleus ReadyStart, Capital VSTAR</b></p> <p>Type Confusion, Improper Validation of Specified Quantity in Input, Out-of-bounds Read, Improper Restriction of Operations within the Bounds of a Memory Buffer, Improper Null Termination, Buffer Access with Incorrect Length Value, Integer Underflow, Improper Handling of Inconsistent Structural Elements</p> <p>Successful exploitation of these vulnerabilities could cause a denial-of-service condition, allow an information leakage, or remote code execution.</p> <p>The following products and versions of the Nucleus RTOS are affected:</p> <ul style="list-style-type: none"> <li>• Capital VSTAR: All versions</li> <li>• Nucleus NET: All versions</li> <li>• Nucleus ReadyStart v3: All versions prior to v2017.02.4</li> <li>• Nucleus ReadyStart v4: All versions prior to v4.1.1</li> <li>• Nucleus Source Code: All versions</li> </ul> <p>Multiple</p> <p>Siemens has released updates for several affected products and recommends updating the latest versions. Siemens recommends countermeasures for products where updates are not available. Siemens has not identified any additional specific workarounds or mitigations.</p> <ul style="list-style-type: none"> <li>• Capital VSTAR: <u>Contact Siemens Customer Support</u> to receive patch and update information.</li> <li>• Nucleus NET: Update to the latest version of Nucleus ReadyStart v3 or v4. <u>Contact Siemens Customer Support</u> or a Nucleus sales team for mitigation advice.</li> <li>• Nucleus ReadyStart v3: <u>Update to v2017.02.4 or later version.</u></li> <li>• Nucleus ReadyStart v4: <u>Update to v4.1.1 or later version.</u></li> <li>• Nucleus Source Code: <u>Contact Siemens Customer Support</u> to receive patch and update information.</li> </ul>	
<p><b>CVSS v3:</b></p> <p><b>Attention:</b></p> <p><b>Vendor:</b></p> <p><b>Equipment:</b></p> <p><b>Vulnerabilities:</b></p>	<p><b>7.3</b></p> <p>Low attack complexity</p> <p><b>mySCADA</b></p> <p><b>myDESIGNER</b></p> <p>Relative Path Traversal</p>	





<b>Risk Evaluation:</b>	Successful exploitation of this vulnerability could allow for remote code execution.
<b>Affected Versions:</b>	The following versions of mySCADA myDESIGNER project creation software is affected: <ul style="list-style-type: none"> <li>myDESIGNER: Versions 8.20.0 and prior</li> </ul>
<b>Sectors:</b>	Energy, Food and Agriculture, Transportation Systems, Water, and Wastewater Systems
<b>Mitigation:</b>	mySCADA recommends users apply update <a href="#">v8.22.0 or later</a> . Upgrade note: RFID card access has been redesigned. If a user uses an RFID card to login, the user will need to re-enter the password for all RFID users in the project after the update is applied.

<b>CVSS v3:</b>	<b>6.5</b>	
<b>Attention:</b>	Exploitable remotely/low attack complexity	
<b>Vendor:</b>	<b>OSIsoft</b>	
<b>Equipment:</b>	<b>PI Vision</b>	
<b>Vulnerabilities:</b>	Cross-site Scripting, Incorrect Authorization	
<b>Risk Evaluation:</b>	Successful exploitation of these vulnerabilities could lead to information disclosure, modification, or deletion.	
<b>Affected Versions:</b>	The following versions of PI Vision, a data management platform, are affected: <ul style="list-style-type: none"> <li>PI:Vision: All versions prior to 2021</li> </ul>	
<b>Sectors:</b>	Multiple Sectors	
<b>Mitigation:</b>	OSIsoft recommends upgrading to PI vision 2021. Information can be found in the <a href="#">OSIsoft PI Vision security bulletin</a> OSIsoft recommends users apply the following workarounds for PI Vision to help reduce risk: <ul style="list-style-type: none"> <li>Configure Publisher and Explorer roles in PI Vision User Access Levels to restrict which users can create or modify displays.</li> <li>Remove any Limits properties from AF child attributes using PI System Explorer or a bulk editing tool.</li> </ul> OSIsoft recommends the following defense measures to lower the impact of exploitation for PI Vision: <ul style="list-style-type: none"> <li>Use a modern web browser such as Microsoft Edge, Google Chrome, or Mozilla FireFox. Do not use Microsoft Internet Explorer.</li> <li>If upgrade is not an option, administrators should regularly audit the AF hierarchy to ensure there are no unexpected or unknown elements, attributes, or attribute properties. It is recommended security on elements in AF be configured and enforced in addition to configuring PI point security.</li> <li>Potential unauthorized viewing of PI System data due to this issue is limited to permissions granted to the PI Vision Application Pool Identity. Configure a dedicated identity</li> </ul>	



mapping for PI Vision servers and manage permissions in accordance with a data classification policy.

**CVSS v3:**

**Attention:**

**Vendor:**

**Equipment:**

**Vulnerabilities:**

**Risk Evaluation:**

**Affected Versions:**

**Sectors:**

**Mitigation:**

**6.9**

Exploitable remotely/low attack complexity

**OSIsoft**

**PI Web API**

Cross-site Scripting

Successful exploitation of this vulnerability could allow a remote authenticated attacker access to sensitive information or deliver false information.

The following versions of PI Web API, a data management platform, are affected:

- All versions of PI Web API 2019 SPI and prior

Multiple Sectors

OSIsoft recommends upgrading to PI Web API 2021. Additional information can be found in the [OSIsoft PI Web API security bulletin](#) (registration required).

OSIsoft recommends applying the following workaround in PI Web API to help reduce the risk:

Remove the OSIsoft.REST.Documentation.dll from the PI Web API installation directory.

- The PI Web API installation directory is available at this registry entry:
  - [\\HKLM\SOFTWARE\PISystem\WebAPI\InstallationDirectory](#)
- The default PI Web API installation directory is:
  - C:\Program Files\PIPC\WebAPI
  - Removing this file will cause built-in documentation to no longer be available. Navigating to the PI Web API endpoint with a browser will result in an error; however, the PI Web API will continue to function as a REST API
- Documentation can be found at the [OSIsoft website](#). Alternately, users are encouraged to limit access to PI Web API built-in documentation to dedicated development environments

OSIsoft recommends users employ the following defense measures to lower the impact of exploitation for PI Web API:

- Avoid adding authentication type “Anonymous” in PI Web API configuration settings to limit exposure to authenticated users only,
- Consider using a web application firewall to block html responses from PI Web API servers,





- Audit the AF hierarchy to ensure there are no unauthorized databases, elements, or attributes,
- For Kerberos authentication configurations, use Group Policy to deny network authentication to PI Server Administrator accounts on the PI Web API server.

**CVSS v3:** 7.8

**Attention:** Low attack complexity

**Vendor:** Advantech

**Equipment:** WebAccess HMI Designer

**Vulnerabilities:** Heap-based Buffer Overflow, Out-of-bounds Write, Improper Restriction of Operation Within the Bounds of a Memory Buffer, Use After Free, Cross-site Scripting



**Risk Evaluation:** Successful exploitation of these vulnerabilities could result in memory corruption, code execution, hijacking of user’s cookie/session tokens, and unintended browser action.

**Affected Versions:** The following versions of Advantech WebAccess HMI Designer are affected:

- WebAccess HMI Designer Versions prior to 2.1.11.0

**Sectors:** Critical Manufacturing, Energy, Water and Wastewater Systems

**Mitigation:** Advantech recommends users update to the latest version of WebAccess HMI Designer v2.1.11.0 Specific questions should be directed to Advantech customer service.

**CVSS v3:** 9.9

**Attention:** Exploitable remotely/low attack complexity

**Vendor:** Siemens

**Equipment:** SIMATIC WinCC

**Vulnerabilities:** Path Traversal, Insertion of Sensitive Information into Log File



**Risk Evaluation:** Successful exploitation of these vulnerabilities could allow local attackers to escalate privileges, and read, write, or delete critical files.

**Affected Versions:** Siemens reports these vulnerabilities affects the following SIMATIC SCADA HMI system products:

- SIMATIC PCS 7 v8.2 and earlier: All versions
- SIMATIC PCS 7 v9.0: All versions
- SIMATIC PCS 7 v9.1: All versions
- SIMATIC WinCC v7.4 and earlier: All versions
- SIMATIC WinCC v7.5: All versions prior to v7.5 SP2 Update 5
- SIMATIC WinCC v15 and earlier: All versions
- SIMATIC WinCC v16: All versions
- SIMATIC WinCC v17: All versions

**Sectors:** Critical Manufacturing

**Mitigation:** Siemens has released updates for several affected products and recommends updating to the latest versions. Siemens is



preparing further updates and recommends specific countermeasures for products where updates are not, or not yet available.

- SIMATIC PCS 7 v9.1: [Install v7.5 SP2 Update 5](#) or later version

Siemens has identified the following specific workarounds and mitigations users can apply to reduce the risk:

- Harden the application’s host to prevent local access by untrusted personnel

For more information about this issue, please see Siemens’s security advisory [SSA-840188](#)

**CVSS v3:**

**Attention:**

**Vendor:**

**Equipment:**

**Vulnerabilities:**

**Risk Evaluation:**

**Affected Versions:**

**Sectors:**

**Mitigation:**

**4.0**

Low attack complexity

**Siemens**

**Mendix**

Use of web browser cache containing sensitive information

Successful exploitation of this vulnerability could allow a local attacker to read cached documents by exploring the browser cache.

The following versions of Mendix, an application platform, are affected:

- Mendix Applications using Mendix 7: All versions prior to v7.23.26
- Mendix Applications using Mendix 8: All versions prior to v8.18.12
- Mendix Applications using Mendix 9: All versions prior to v9.6.1

Multiple Sectors

Siemens recommends upgrading to the latest version of Mendix:



- Mendix Applications using Mendix 7: [Update to v7.23.26](#) or later
- Mendix Applications using Mendix 8: [Update to v8.18.12](#) or later
- Mendix Applications using Mendix 9: [Update to v9.6.1 or v9.7.0](#) or later

Siemens has identified the following specific workarounds and mitigations users can apply to reduce the risk:

- Applications built with affected versions of Mendix Studio Pro: avoid using file documents that contain sensitive information
- For additional information, please refer to Siemens Security Advisory [SSA-338732](#).





<p><b>CVSS v3:</b></p> <p><b>Attention:</b></p> <p><b>Vendor:</b></p> <p><b>Equipment:</b></p> <p><b>Vulnerabilities:</b></p> <p><b>Risk Evaluation:</b></p> <p><b>Affected Versions:</b></p> <p><b>Sectors:</b></p> <p><b>Mitigation:</b></p>	<p><b>5.3</b></p> <p>Exploitable remotely</p> <p><b>Siemens</b></p> <p><b>Mendix Studio Pro</b></p> <p>Incorrect Authorization</p> <p>Successful exploitation of these vulnerabilities could allow authenticated attackers to manipulate the content of specific objects or to retrieve a specific attribute of arbitrary objects.</p> <p>Siemens reports these vulnerabilities affect the following Mendix products:</p> <ul style="list-style-type: none"> <li>• Mendix Applications using Mendix 8: All versions prior to v8.18.13</li> <li>• Mendix Applications using Mendix 9: All versions prior to v9.6.2</li> </ul> <p>Critical Manufacturing</p> <p>Mendix has released updates for the affected product lines and recommends updating to the latest versions and redeploying the applications.</p> <p>Mendix Applications using Mendix 8: <u>Update to v8.18.13</u> or later version and redeploy the application.</p> <ul style="list-style-type: none"> <li>• Mendix Applications using Mendix 9: <u>Update to v9.6.2 or v9.7.0</u> or later version and redeploy the application.</li> </ul> <p>Siemens has identified the following specific workarounds and mitigations users can apply to reduce the risk:</p> <ul style="list-style-type: none"> <li>• In applications built with affected versions of Mendix Studio Pro, avoid using file documents that contain sensitive information.</li> </ul> <p>For more information about these vulnerabilities, please see Siemens’s security advisory <a href="#">SSA-779699</a></p>	
<p><b>CVSS v3:</b></p> <p><b>Attention:</b></p> <p><b>Vendor:</b></p> <p><b>Equipment:</b></p> <p><b>Vulnerabilities:</b></p> <p><b>Risk Evaluation:</b></p> <p><b>Affected Versions:</b></p> <p><b>Sectors:</b></p> <p><b>Mitigation:</b></p>	<p><b>9.8</b></p> <p>Exploitable remotely/low attack complexity</p> <p><b>Siemens</b></p> <p><b>SCALANCE W1750D</b></p> <p>Improper Restriction of Operations Within the Bounds of a Memory Buffer, Command Injection, Path Traversal</p> <p>Successful exploitation of these vulnerabilities could allow an attacker to execute code on the affected devices, read arbitrary files, or create a denial-of-service condition.</p> <p>The following versions of SCALANCE W1750D, a wireless access point, are affected:</p> <ul style="list-style-type: none"> <li>• SCALANCE W1750D: All versions prior to v8.7.1.3</li> <li>• SCALANCE W1750D: Versions 8.7.1.3 and newer (only affected by CVE-2021-37727, CVE-2021-37730, and CVE-2021-37734)</li> </ul> <p>Multiple Sectors</p> <p>Siemens recommends upgrading their products to the latest version:</p>	



SCALANCE W1750D: [Update to v8.7.1.3](#) or later.

Siemens has identified the following specific workarounds and mitigations users can apply to reduce the risk:

- Block access to the Aruba Instant Command Line Interface from all untrusted users.
- Block access to the Aruba Instant web-based management interface from all untrusted users.
- Enable the Enhanced PAPI Security feature, where available, to prevent exploitation of these vulnerabilities. For assistance from the Siemens Technical Assistance Center (TAC), please [contact Siemens](#) (login required).
- Block access for Aruba Instant device on Port UDP/8211 from all untrusted users.

For additional information, please refer to Siemens Security Advisory [SSA-917476](#)

**CVSS v3:**

**Attention:**

**Vendor:**

**Equipment:**

**Vulnerabilities:**

**Risk Evaluation:**

**Affected Versions:**

**Sectors:**

**Mitigation:**

**9.8**

Exploitable remotely/low attack complexity

**Siemens**

**Nucleus RTOS based APOGEE and TALON Products**



Type Confusion, Improper Validation of Specified Quantity in Input, Out-of-bounds Read, Improper Restriction of Operations within the Bounds of a Memory Buffer, Improper Null Termination, Buffer Access with Incorrect Length Value, Integer Underflow, Improper Handling of Inconsistent Structural Elements

Successful exploitation of these vulnerabilities could allow denial-of-service conditions, remote code execution, information leaks, and out-of-bounds reads and writes.

The following Nucleus RTOS based APOGEE and TALON Products, direct digital control (DDC) devices, are affected:

- APOGEE MBC (PPC) (BACnet): All versions
- APOGEE MBC (PPC) (P2 Ethernet): All versions
- APOGEE MEC (PPC) (BACnet): All versions
- APOGEE MEC (PPC) (P2 Ethernet): All versions
- APOGEE PXC Compact (BACnet): All versions
- APOGEE PXC Compact (P2 Ethernet): All versions
- APOGEE PXC Modular (BACnet): All versions
- APOGEE PXC Modular (P2 Ethernet): All versions
- TALON TC Compact (BACnet): All versions
- TALON TC Modular (BACnet): All versions

Critical Manufacturing

Siemens has identified and recommended the following specific workarounds and mitigations users can apply to reduce the risk:



- Restrict system access to authorized personnel and follow a least privilege approach.
- Disable the DHCP client and use static IP address configuration instead.
- Protect network access to the affected devices with appropriate measures, (e.g., firewalls) to reduce the risk.
- Disable FTP on all devices.
- Apply appropriate strategies for mitigation on the network level to ensure affected devices are as segmented.
- Ensure default passwords are changed.
- Implement defence in depth concepts to mitigate risk of an attacker gaining access to affected devices and networks.
- Contact a Siemens’s office for support.

For more information see Siemens Security Advisory [SSA-114589](#).

**CVSS v3:**

**Attention:**

**Vendor:**

**Equipment:**

**Vulnerabilities:**

**Risk Evaluation:**

**Affected Versions:**

**Sectors:**

**Mitigation:**

**7.8**

Low attack complexity

**Siemens**

**NX**

Use After Free, Access of Uninitialized Pointer

Successful exploitation of these vulnerabilities could lead to an access violation and arbitrary code execution on the target system.

Siemens reports these vulnerabilities affects the following NX products:

- NX 1953 Series: All versions prior to v1973.3700
- NX 1980 Series: All versions prior to v1988

Critical Manufacturing

Siemens has released updates for the NX and recommends updating to the latest version.

- NX 1953 Series: Update to v1973.3700 or later version
- NX 1980 Series: Update to v1988 or later version

Siemens recommends users avoid opening of untrusted files from unknown sources.

For more information about this issue, please see Siemens’s security advisory [SSA-328042](#).





**CVSS v3:** **6.4**  
**Attention:** Exploitable remotely  
**Vendor:** **Siemens**  
**Equipment:** **Climatix POL909 (AWM module)**  
**Vulnerabilities:** Missing Encryption of Sensitive Data  
**Risk Evaluation:** Successful exploitation of this vulnerability could allow sensitive data disclosure or modification of data in transit.  
**Affected Versions:** The following versions of Climatix POL909 (AWM module), an advanced web module, are affected:



- Climatix POL909 (AWM module): All versions prior to v11.34

**Sectors:** Critical Manufacturing  
**Mitigation:** Siemens recommends users [update to v11.34](#) or later version. Siemens has not identified any additional specific workarounds or mitigations. For additional information, please refer to Siemens Security Advisory [SSA-703715](#)

**CVSS v3:** **7.8**  
**Attention:** Low attack complexity  
**Vendor:** **Siemens**  
**Equipment:** **SETRON powermanager**  
**Vulnerabilities:** Incorrect Permission Assignment for Critical Resource  
**Risk Evaluation:** Successful exploitation of this vulnerability could allow an authenticated local attacker to inject arbitrary code and escalate privileges.



**Affected Versions:** The following versions of Siemens SETRON powermanager, a power monitoring software to analyze energy consumption, are affected:

- SETRON powermanager Version 3: All versions

**Sectors:** Critical Manufacturing  
**Mitigation:** Siemens has released a security patch for [SETRON powermanager v3.6 HF1](#) and recommends updating to the latest version. Siemens recommends users also harden the application server to prevent local access by untrusted personnel. For more information about this issue and the mitigations, please see Siemens security advisory [SSA-537983](#).

**CVSS v3:** **7.8**  
**Attention:** Low attack complexity  
**Vendor:** **WECON**  
**Equipment:** **PLC Editor**  
**Vulnerabilities:** Stack-based Buffer Overflow, Out-of-bounds Write  
**Risk Evaluation:** Successful exploitation of these vulnerabilities may allow arbitrary code execution.  
**Affected Versions:** The following versions of PLC Editor ladder logic software are affected:







<b>Sectors:</b>	<ul style="list-style-type: none"> <li>• PLC Editor: Versions 1.3.8 and prior</li> </ul>
<b>Mitigation:</b>	<p>Critical Manufacturing, Energy, Water and Wastewater Systems</p> <p>WECON has not responded to requests to work with CISA to mitigate these vulnerabilities. Users of these affected products are invited to contact <a href="#">WECON technical support</a> for additional information.</p> <p>CISA also recommends users take the following measures to protect themselves from social engineering attacks:</p> <ul style="list-style-type: none"> <li>• Do not click web links or open unsolicited attachments in email messages.</li> <li>• Refer to <a href="#">Recognizing and Avoiding Email Scams</a> for more information on avoiding email scams.</li> <li>• Refer to <a href="#">Avoiding Social Engineering and Phishing Attacks</a> for more information on social engineering attacks.</li> </ul>
<b>CVSS v3:</b>	<b>8.6</b>
<b>Attention:</b>	Exploitable remotely/low attack complexity
<b>Vendor:</b>	<b>Eclipse, eProxima, GurumNetworks, Object Computing, Inc. (OCI), Real-Time Innovations (RTI), TwinOaks Computing</b>
<b>Equipment:</b>	<b>CycloneDDS, FastDDS, GurumDDS, OpenDDS, Connex DDS Professional, Connex DDS Secure, Connex DDS Micro, CoreDX DDS</b>
<b>Vulnerabilities:</b>	<p>Write-what-where Condition, Improper Handling of Syntactically Invalid Structure, Network Amplification, Incorrect Calculation of Buffer Size, Heap-based Buffer Overflow, Improper Handling of Length Parameter Inconsistency, Amplification, Stack-based Buffer Overflow</p> <p>CISA is aware of a public report detailing vulnerabilities found in multiple open-source and proprietary Object Management Group (OMG) Data-Distribution Service (DDS) implementations. This advisory addresses a vulnerability that originates within, and affects the implementation of, the DDS standard. In addition, this advisory addresses other vulnerabilities found within the DDS implementation.</p>
<b>Risk Evaluation:</b>	<p>Successful exploitation of these vulnerabilities could result in denial-of-service or buffer-overflow conditions, which may lead to remote code execution or information exposure.</p>
<b>Affected Versions:</b>	<p>The following implementations of OMG DDS are affected:</p> <ul style="list-style-type: none"> <li>• Eclipse CycloneDDS: All versions prior to 0.8.0</li> <li>• eProxima Fast DDS: All versions prior to 2.4.0 (#2269)</li> <li>• GurumNetworks GurumDDS: All versions</li> <li>• Object Computing, Inc. (OCI) OpenDDS: All versions prior to 3.18.1</li> <li>• Real-Time Innovations (RTI) Connex DDS Professional and Connex DDS Secure: Versions 4.2x to 6.1.0</li> <li>• RTI Connex DDS Micro: Versions 3.0.0 and later</li> <li>• TwinOaks Computing CoreDX DDS: All versions prior to 5.9.1</li> </ul>





**Sectors:**

Multiple

**Mitigation:**

Eclipse recommends users apply the [latest CycloneDDS patches](#).

eProsima recommends users apply the [latest Fast DDS patches](#).

CISA reached out to Gurum Networks but did not respond to requests for coordination. Users should [contact GurumNetworks](#) for assistance.

OCI recommends users update to [Version 3.18.1](#) of OpenDDS or later.

RTI recommends users apply the available patches for these issues. A

patch is available on the [RTI customer portal](#) or by contacting RTI

Support. Also, contact [RTI Support](#) for mitigations, including how to use

RTI DDS Secure to mitigate against the network amplification issue

defined by [CVE-2021-38487](#)

Twin Oaks Computing recommends users apply CoreDX DDS Version

5.9.1 or later, which can be downloaded on the [Twin Oaks website](#)

(login required).

*C5 Technology*

*Cyber Security Team*