

- [Risk Management](#)
- [Compliance](#)
- [Privacy](#)
- [Supply Chain](#)
- ▼ [Security Architecture](#)
 - [Cloud Security](#)
 - [Identity & Access](#)
 - [Data Protection](#)
 - [Network Security](#)
 - [Application Security](#)
- ▼ [Security Strategy](#)
 - [Risk Management](#)
 - [Security Architecture](#)
 - [Disaster Recovery](#)
 - [Training & Certification](#)
 - [Incident Response](#)
- [ICS/OT](#)
- [IoT Security](#)

[Home](#) > [ICS/OT](#)



Hackers Can Make Siemens Building Automation Controllers 'Unavailable for Days'

By [Eduard Kovacs](#) on May 13, 2022

Share

发推

推荐 0



A vulnerability affecting building automation controllers from Siemens can be exploited to disrupt a device for an extended period of time, according to OT and IoT cybersecurity firm Nozomi Networks.

Nozomi researchers recently analyzed Siemens' PXC4.E16, a programmable building automation system (BAS) of the Desigo family that is designed for HVAC and building service plants.

They discovered that the device, specifically its ABT Site Engineering and Commissioning Tool, is affected by a vulnerability that can be exploited for denial-of-service (DoS) attacks.

The vulnerability has a severity rating of "medium" based on its CVSS score, but cybersecurity experts have often warned that in industrial environments a DoS attack can have a major impact.

The flaw, identified as CVE-2022-24040, is related to the use of the PBKDF2 key derivation function for securing user passwords. A malicious insider or an attacker who has "user profile access" privileges to the tool can create or update an account and cause a DoS condition by attempting to log in to that account.

"The web application fails to enforce an upper bound to the cost factor of the PBKDF2 derived key during the creation or update of an account," Siemens explained in its [advisory](#). "An attacker with

the user profile access privilege could cause a denial of service (DoS) condition through CPU consumption by setting a PBKDF2 derived key with a remarkably high cost effort and then attempting a login to the so-modified account.”

The tests conducted by Nozomi showed that, in a worst-case scenario, an attacker could “make the device unavailable for days just by attempting a login,” and they could repeat the process to further extend the controller’s downtime.



“It is also possible that threat actors can attack BAS while simultaneously launching a catastrophic attack on other industrial control systems (ICS) within a facility. If the fire alarm system or other systems are DDoSed, it could intensify a cyber-physical attack,” Nozomi [warned](#).

[Siemens patched the vulnerability](#) this week, along with six other flaws affecting its Desigo PXC and DXR devices.

Related: [New Vulnerabilities Can Allow Hackers to Remotely Crash Siemens PLCs](#)

Related: [Siemens Addresses Over 90 Vulnerabilities Affecting Third-Party Components](#)

Related: [Many IoT Devices Exposed to Attacks Due to Unpatched Flaw in uClibc Library](#)

Share

发推

推荐 0



Eduard Kovacs ([@EduardKovacs](#)) is a contributing editor at SecurityWeek. He worked as a high school IT teacher for two years before starting a career in journalism as Softpedia’s security news reporter. Eduard holds a bachelor’s degree in industrial informatics and a master’s degree in computer techniques applied in electrical engineering.

Previous Columns by Eduard Kovacs:

[Hackers Can Make Siemens Building Automation Controllers 'Unavailable for Days'](#)

[Critical Vulnerability Allows Remote Hacking of Zyxel Firewalls](#)

[Critical Vulnerabilities Provide Root Access to InHand Industrial Routers](#)

[Size of Early Stage Cyber Deals Continues to Surge: DataTribe](#)

[Hundreds of Thousands of Konica Printers Vulnerable to Hacking via Physical Access](#)

[Virtual Event Series - Security Summit Online Events by SecurityWeek](#)

sponsored links

[2022 ICS Cyber Security Conference | USA \[Hybrid: Oct. 24-27\]](#)

[2022 CISO Forum: September 13-14 - A Virtual Event](#)

[2022 Singapore/APAC ICS Cyber Security Conference](#)

 **Tags:**

[ICS/OT](#)

[NEWS & INDUSTRY](#)

[Vulnerabilities](#)

Search

Get the Daily Briefing