Microsoft finds vulnerabilities it says could be used to shut down power plants

Rockwell Automation

reader comments

33 with

On Friday, Microsoft disclosed 15 high-severity vulnerabilities in a widely used collection of tools used to program operational devices inside industrial facilities such as plants for power generation, factory automation, energy automation, and process automation. The company warned that while exploiting the code-execution and denial-of-service vulnerabilities was difficult, it enabled threat actors to "inflict great damage on targets."

The vulnerabilities affect the CODESYS V3 software development kit. Developers inside companies such as Schneider Electric and WAGO use the platform-independent tools to develop programmable logic controllers, the toaster-sized devices that open and close valves, turn rotors, and control various other physical devices in industrial facilities worldwide. Specifically, the SDK allows developers to make PLCs compatible with IEC 611131-3, an international standard that defines programming languages that are safe to use in industrial environments. Examples of devices that use CODESYS V3 include Schneider Electric's Modicon TM251 and the WAGO PFC200.

“A DOS attack against a device using a vulnerable version of CODESYS could enable threat actors to shut down a power plant, while remote code execution could create a backdoor for devices and let attackers tamper with operations, cause a PLC to run in an unusual way, or steal critical information,” Microsoft researchers wrote. Friday’s advisory went on to say:

> *With CODESYS being used by many vendors, one vulnerability may affect many sectors, device types, and verticals, let alone multiple vulnerabilities. All the vulnerabilities can lead to DoS and 1 RCE. While exploiting the discovered vulnerabilities requires deep knowledge of the proprietary protocol of CODESYS V3 as well as user authentication (and additional permissions are required for an account to have control of the PLC), a successful attack has the potential to inflict great damage on targets. Threat actors could launch a DoS attack against a device using a vulnerable version of CODESYS to shut down industrial operations or exploit the RCE vulnerabilities to deploy a backdoor to steal sensitive data, tamper with operations, or force a PLC to operate in a dangerous way.*

Microsoft privately notified Codesys of the vulnerabilities in September, and the company has since released patches that fix the vulnerabilities. It’s likely that by now, many vendors using the SDK have installed updates. Any who haven’t should make it a priority.

Advertisement

Microsoft said exploiting the vulnerabilities required a deep knowledge of Codesys’ proprietary protocol. It also requires attackers clear a tall hurdle in the form of gaining authentication to a vulnerable device. One way to achieve authentication is to exploit an already patched vulnerability tracked as CVE-2019-9013 in the event a PLC hasn’t yet been patched against it.

While the vulnerabilities are difficult to exploit, threat actors have been able to pull off such attacks in the past. Malware tracked as Triton and Trisis have been used in at least two critical facilities. The malware, attributed to the Kremlin, is designed to disable safety systems that detect and remediate unsafe conditions.

Such attacks are rare, however. Combined with the likelihood that the 15 vulnerabilities are patched in most previously vulnerable production environments, the dire consequences Microsoft is warning of appear unlikely.

In an email received after this post went live on Ars, Jimmy Wylie and Sam Hanson, technical lead malware analyst and senior vulnerability analyst at industrial control security firm Dragos, provided this assessment of the vulnerabilities:

> *Given CODESYS's market share and cross-industry customer base, vulnerabilities like these discovered by Microsoft, should be taken seriously by customers and vendors alike. That said, CODESYS isn't widely used in power generation so much as discrete manufacturing and other types of process control. So that in itself should allay some concern when it comes to the potential to "shut down a power plant".*
>
> *When looking specifically at these vulnerabilities and the published advisory from CODESYS, they all require authentication for successful exploitation. But if an adversary is authenticated (has the username and password) to your PLC, you've got bigger problems than these CVEs, and they can do all kinds of things that make the CVEs unnecessary.*
>
> *Either way, simply having an RCE or DOS exploit isn't the same as having the ability to shut down a power plant or say, make specific changes to a manufacturing process. For example, the TRISIS attack in 2017 included a 0-day exploit for that safety controller, and while we know the attackers*

> *were there for quite some time, they were never able to do anything truly disastrous, beyond some financial consequences. The reason is that industrial systems are extremely complex, and being able to access one part doesn’t necessarily mean the whole thing will come crashing down. These things aren’t wobbly jenga towers, where one brick means imminent collapse. They’re more like skyscrapers engineered for resiliency against a variety of factors like wind and earth quakes.*

The vulnerabilities are tracked as:

Codesys on Friday issued its own advisory, and Microsoft has made code available here that helps organizations identify any vulnerable devices that may still be in use.

https://arstechnica.com/?p=1960538