Beat: Technology

Kaspersky Lab discovers critical vulnerabilities in popular industrial protocol

Affecting products from multiple vendors

Jeddah - Saudi Arabia, 24.05.2018, 20:18 Time

USPA NEWS - Kaspersky Lab ICS CERT has analyzed the OPC UA (Object Linking and Embedding for Process Control Unified Automation) protocol, which is designed for secure data transfer between servers and clients in industrial systems, including critical infrastructure. Analysis discovered 17 zero-day vulnerabilities in the protocol´s implementation, leading to denial-of-service threat attacks, as well as remote code execution. In addition, several flaws were found in commercial products built on the protocol. All vulnerabilities were reported to the developers and were fixed by the end of March 2018.

OPC UA is an industrial protocol, which was developed and released by the OPC Foundation in 2006 for reliable and secure data transmission between various systems on an industrial network. This protocol is widely used by major vendors in modern industrial facilities, in the manufacturing, oil and gas, pharmaceuticals industries and others. Its gateways are installed by a growing number of industrial enterprises, for communication in automated process control and telemetry, and monitoring and telecontrol systems, allowing these enterprises to unify their management processes. The protocol is also used in IIoT and smart city components, which are increasingly attracting hacker attention.
Kaspersky Lab ICS CERT experts analyzed OPC UA architecture and its products. They examined its open-source code (available on GitHub), including a sample sever, and discovered that current implementations of the protocol had code design and writing errors. These errors should not exist in such widespread critical infrastructure software. Overall, 17 zero-day vulnerabilities in the OPC Foundation´s products were identified and reported to the developers, who fixed them accordingly.

In addition, Kaspersky Lab ICS CERT analyzed third-party software based on this industrial protocol, including solutions by leading industry vendors. In most cases, they discovered flaws were caused by the developers not using some of the protocol implementation functions properly. In other cases, vulnerabilities were the result of incorrect modifications applied to the protocol´s infrastructure. Thus, experts discovered the insecure implementation of functions in a commercial product, despite the fact that the original OPC Foundation implementation did not include errors. As a result, such modifications in the protocol´s logic, made by vendors for unknown reasons, was leading to risky functionality.
All the vulnerabilities found in the OPC UA protocol implementations could result in heavy damage to industry. On the one hand there was the risk of denial-of-service (DoS) issues, which could pose serious threats to industrial systems by disrupting or shutting down industrial processes. On the other hand, remote code execution was made possible, allowing attackers to send any kind of server commands to control industrial processes, or continue their intrusion into the network.

“Very often software developers put too much trust in industrial protocols, and implement the technology in their solutions without putting the product code through security checks. Thus, vulnerabilities in the example used can affect complete product lines, so it´s highly important that vendors pay close attention to such widely available technologies. Moreover, they should not be deceived by the idea that they can design their own piece of software. Many think this could be more efficient and secure than existing software, but even a brand new piece of software may still contain numerous vulnerabilities.“ said Sergey Temnikov, Senior security researcher at Kaspersky lab ICS CERT.
Kaspersky Lab recommends organizations:
“¢ pay close attention to security checks and testing as a necessary step during the application development process, and do not fully rely on protocols.
“¢ conduct audits and pen testing to discover vulnerabilities.
“¢ isolate software development processes, therefore if an application is hacked, attackers won´t be able to get access to the network.

About Kaspersky Lab
Kaspersky Lab is a global cybersecurity company, which has been operating in the market for over 20 years. Kaspersky Lab´s deep threat intelligence and security expertise is constantly transforming into next generation security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company´s comprehensive security portfolio

includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky Lab technologies and we help 270,000 corporate clients protect what matters most to them.

About Kaspersky Lab ICS CERT
Kaspersky Lab Industrial Control Systems Cyber Emergency Response Team (Kaspersky Lab ICS CERT) is a global project launched by Kaspersky Lab in 2016 to coordinate the efforts of automation system vendors, industrial facility owners and operators, and IT security researchers to protect industrial enterprises from cyberattacks. Kaspersky Lab ICS CERT devotes its efforts primarily to identifying potential and existing threats that target industrial automation systems and the Industrial Internet of Things. During its first year of operation, the team identified over 110 critical vulnerabilities in products by major global ICS vendors. Kaspersky Lab ICS CERT is an active member and partner of leading international organizations that develop recommendations on protecting industrial enterprises from cyberthreats. ics-cert.kaspersky.com

Article online:
https://www.uspa24.com/bericht-13442/kaspersky-lab-discovers-critical-vulnerabilities-in-popular-industrial-protocol.html

Editorial office and responsibility:
V.i.S.d.P. & Sect. 6 MDStV (German Interstate Media Services Agreement): Zayad Alshaikhli

Exemption from liability:
The publisher shall assume no liability for the accuracy or completeness of the published report and is merely providing space for the submission of and access to third-party content. Liability for the content of a report lies solely with the author of such report. Zayad Alshaikhli

Editorial program service of General News Agency:
United Press Association, Inc.
3651 Lindell Road, Suite D168
Las Vegas, NV 89103, USA
(702) 943.0321 Local
(702) 943.0233 Facsimile
info@unitedpressassociation.org
info@gna24.com
www.gna24.com