Cyberthreats are escalating; safeguard your systems with Eaton

Eaton's Gigabit Network Card is the first UPS connectivity device to meet both UL 2900-1 and IEC 62443-4-2 cybersecurity standards.

Global reliance on the Java Log4j library left IT departments around the world scrambling to patch or mitigate a vulnerability that was identified in December 2021. This was just the latest in an ever-increasing series of malicious threats. The vulnerability forced nearly 4,000 federal, provincial and municipal web sites throughout Canada to shut down for several days while IT staffs scanned for possible vulnerabilities. And with an estimated 4.6 billion global devices utilizing Java, it's not a matter of ***if*** this will happen again, it's ***when***. That's why leveraging the Eaton Network-M2 Card in your government applications represents a critical measure in your overall cybersecurity strategy.

What is Log4j?

Log4j is a Java-based logging utility affected by the internet vulnerability Log4Shell. Affecting millions of computers, Log4Shell is considered to be among the most serious vulnerabilities. With the ability to record activities on a wide range of computer systems, Log4Shell enables cybercriminals to steal sensitive information, take control of targeted systems and slip malicious content to other users communicating with the affected server.

What *wasn't* affected in the breach? The Eaton Network-M2 Card

Following the December incident, numerous governmental departments reached out to Eaton to see if any of their UPSs or PDUs had been impacted. The answer was a resounding **NO**. Here's why organizations looking to bullet-proof their cybersecurity strategy can count on the Eaton Network-M2 Card as one of the strongest links in the chain of protection:

- The first UPS connectivity device to meet the UL 2900-1 cybersecurity standard and IEC 62443-4-2 certification
- By default, only essential services run on the card and all communication is encrypted and certificate-based
- The firmware itself is encrypted – preventing attackers from analyzing its structure –and the file is signed, making it impossible to apply altered or corrupted versions
- Access to the card requires authorization credentials and all users are assigned role-based permissions
- Eaton continually evaluates ongoing security threats and quickly releases security patches

Powering Business Worldwide

Why trust Eaton for cybersecurity?

Because cybersecurity incidents can cripple an organization in minutes, customers need partners who are dedicated to the highest cybersecurity standards. Eaton goes above and beyond, evidenced by:

- Cybersecurity is at the core of our "secure by design" philosophy, and embedded in all the Intelligent Power products and platforms we bring to market
- Eaton partners with the National Renewable Energy Laboratory (NREL) to further research initiatives to address the security gap at the edge-level of the power system
- Our commitment to establishing cyber-secure processes is underscored by our Product Cybersecurity Center of Excellence, where experts discover new ways to help protect products and systems against cyberattack, provide internal training, and help customers deploy and maintain secure solutions
- Eaton introduced the first research and testing facility approved to participate in UL's Cybersecurity Client Lab Validation program in Pittsburgh, Penn., with a second lab added in Pune, India
- We collaborate with renowned standards leader, Underwriters Laboratories (UL), to establish measurable cybersecurity criteria for network-connected power management products and systems

Simple steps to help safeguard against cyberthreats:

- Encrypt and replicate your data
- Update your systems/firmware
- Educate your staff
- Utilize digital certificates
- Learn to recognize phishing attempts

Powering Business Worldwide

To learn more, please visit:
Eaton.com/Network-M2