Xylem Security Advisory

Cybersecurity and Infrastructure Security Agency (CISA) - "Shields Up" Advisory (v2.0)

February 16, 2022 (February 28, 2022)

Overview

In response to heightened tensions between Russia and Ukraine, CISA has issued a "Shields Up" advisory to every organization in the United States, including federal agencies.

The Shields Up Advisory provides steps organizations can take immediately to ensure that:

- The likelihood of a damaging cyber intrusion is reduced
- A potential intrusion is quickly detected
- An organization is prepared to respond if an intrusion does occur, and;
- An organization has maximized their resilience in the face of a destructive cyber incident

Additionally, be on the lookout for any activity from some of the notable threat clusters such as:

- Drangonfly 2.0
- Sandworm Team
- Temp.Veles

Xylem recommends all customers adopt a heightened posture when it comes to cybersecurity and protecting critical assets.

References
- CISA: Shields Up Advisory
- CISA: Shields Up Technical Guidance
- CISA: Destructive Malware Targeting Organizations in Ukraine
- CISA: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure
- CISA: Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats
- CISA: Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure
- CISA: Preparing for and Mitigating Potential Cyber Threats
- CISA: Russia Cyber Threat Overview Advisories
- Xylem Security Advisories

Contact Information

For any questions related to this Xylem Security Advisory or to report a security concern, please contact product.security@xylem.com.

Disclaimer

This document is provided on an as-is basis and does not imply any kind of guarantee or warranty, including the warranties of merchantability or fitness for a particular use. Use of the information in the document or materials linked from the document is at your own risk. Xylem reserves the right the change or update this document any time.

Revision History	
Version	**Updates**
1.0	Initial draft
2.0	Added details for potential threat actors and added additional CISA references.