Date: 2018-11-16

NOTICE OF DATA BREACH

What Happened?	OSIsoft is experiencing a security incident that may affect employees, interns, consultants and contractors. Stolen credentials were used to remotely access OSIsoft computers. OSIsoft intrusion detection systems alerted IT to unauthorized activity. Our security service provider has recovered direct evidence of credential theft activity involving 29 computers and 135 accounts. We have concluded, however, that all OSI domain accounts are affected.
What Information Was Involved?	You should assume your OSI domain logon account name, as well as email address and password have been compromised. Although Active Directory (AD) uses cryptographic protection methods, your personal credentials may have been breached. If you configured your external accounts to use OSIsoft email address for password recovery, re-used a previous OSIsoft password, or there is a systemic pattern with external accounts, you are at a higher risk of credential theft.
What We Are Doing.	We continue to investigate the security incident with our security service providers in order to learn more and prevent similar incidents from occurring in the future. We have also developed a comprehensive remediation strategy that includes a contingency plan, in case there is an escalation of unauthorized activity as the investigation continues. Further, we have applied important security measures to our systems to help safeguard our environment and protect your personal information. As part of these measures, we are expediting our MFA (multifactor authentication) security solution as a foundational step to protect OSIsoft assets from unauthorized external use.
What You Can Do.	Take a moment to review OSIsoft security practices found on OSIsoft.Home under IT department information. Be vigilant, Information Security is a shared duty. Report suspicious activity to IT System Managers. Criminals with stolen credentials could target your banking, e-commerce and other online accounts, if passwords were re-used or stored on your system. You should reset external accounts to use passwords that are different from your OSI domain account password.

	Wait for advice from IT System Managers on coordinated reset of all OSIsoft passwords. Disable or restrict remote desktop and file sharing on the computers you manage including test machines. Periodically review system logs and verify the purpose of any remote logons.
Other Important Information. This notification references an ongoing investigation. We will keep you informed of specific actions and policies designed to protect you, your colleagues, our company assets and our greater community of interest.	
For More Information.	Contact a member of the OSIsoft Incident Response Task Force if you have questions or concerns: Brian Bostwick, Bryan Owen, Darius Card, Harry Paul, and Mike Lemley. Call [1 510 297 5828] or go to [https://techsupport.osisoft.com/Contact-Us]