Tridium To Post Security Patch

February 6, 2013

The purpose of this message is to alert you that Tridium will be posting a security patch no later than Wednesday, February 13 for NiagaraAX Framework software versions 3.5, 3.6 and 3.7. We will issue a Security Alert announcement as soon as the patch is ready for download from Niagara Central.

The patch addresses a new vulnerability to NiagaraAX systems that was publicly disclosed earlier this week at a security analyst conference by two security researchers – Billy Rios and Terry McCorkle. During the conference Rios and McCorkle successfully demonstrated that with a valid user account or guest privileges enabled they were able to use the vulnerability in the system to escalate their system privileges on a NiagaraAX system.

The researchers had informed Tridium of this vulnerability in late December 2012 and we immediately began developing a solution. Our roll-out plan, undertaken in cooperation with the researchers and ICS-Cert, was to incorporate the patch in a scheduled update of the software for midMarch.However, in light of recent publicity about the issue we have accelerated the release of the patch and want to alert the user community of the timing.

Our forthcoming Security Alert will include more details about the vulnerability, a software download to fix the problem and clear instructions on how to apply it. **We strongly recommend that all system integrators and customers apply the patch to their NiagaraAX systems.**

Tridium recognizes that the security of control systems is a No. 1 concern for customers. This incident again underscores the need for all Niagara Framework customers and system integrators to review their security policies to ensure their Internet-facing systems are properly protected. We continue to recommend to all customers that Niagara Framework systems operate behind a firewall or VPN. While the vast majority of installed Niagara systems do, there remain many that are not adequately protected, as Mr. Rios and Mr. McCorkle have shown. We share their concern about the importance of addressing this issue.