Tridium Issues Security Patch

February 11, 2013

All customers should apply patch to existing NiagaraAX 3.5, 3.6 or 3.7 systems

Tridium is releasing a security patch for NiagaraAX 3.5, 3.6 and 3.7 that addresses the vulnerability associated with the Security Bulletin that Tridium issued on February 6, 2013. The Security Patch is now available. The patch removes a directory traversal vulnerability allowing a user with a valid user account or guest privileges to escalate his or her privileges on a NiagaraAX system.

Tridium strongly recommends all customers apply the security patch to any existing 3.5, 3.6 or 3.7 systems to correct this vulnerability. Customers with systems running a version of NiagaraAX released prior to 3.5 should purchase an upgrade to the latest version of the Niagara Framework software in order to take advantage of the latest security improvements.

The security patch along with details about the patch and installation instructions are available on Niagara Central at:
https://www.niagaracentral.com/ord?portal:/dev/wiki/Niagara_AX_Security_Patch_11-Feb-2013.
(Niagara Central access required)

The patch does not affect any standard Niagara configuration or functionality. The only impact of the change is to remove the vulnerability.

It is important all Niagara Framework customers and system integrators 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. Tridium understands the importance of providing a securable software framework to its customers. Whenever critical security issues are discovered, Tridium is committed to taking the appropriate steps to resolve them quickly.