InterSystems Official
Andreas Dieckow · Mar 10, 2016

Advisory: Cross-Protocol Attack on TLS Using SSLv2 (DROWN)

This advisory concerns the recently announced vulnerability CVE-2016-0800, aka DROWN, which is due to weaknesses in SSLv2. For more information, see https://drownattack.com. This vulnerability may be relevant to InterSystems customers as InterSystems products have the capability to utilize SSLv2.

SSLv2 is known to have weak security and it has long been recommended that it be disabled in installations. SSLv2 has always been disabled by default in all released versions of InterSystems products.

If your organization uses the default configuration for its instances, then no action is required. However, if your organization has enabled SSLv2 for any of its instances, then to eliminate this vulnerability you must disable it. This is especially critical if any instances share a private key. (Note that InterSystems always strongly discourages sharing private keys due to its inherent dangers.) Your organization ’ s administrators can use the Management Portal or the command line utilities to make the required modifications to SSL/TLS configurations of InterSystems product instances.

If you have any questions regarding this alert, please contact the InterSystems Worldwide Response Center.

#InterSystems Official

Source URL:https://community.intersystems.com/post/advisory-cross-protocol-attack-tls-using-sslv2-drown