技術ノート KGTN 2014110401

現 象

[GGH4.X] GG のセッションは SSL 3.0 の脆弱性「POODLE」の影響はあるのか？

説 明

GG のセッションは SSL 2.0 を使用しておりますので，脆弱性 POODLE（Padding Oracle On Downgraded Legacy Encryption）の影響はありません．なお，GG の Ver.5 から TLS 1.2 がサポートされる見込みです．

Last reviewed: Nov 04, 2014
Status: DRAFT
Ref: CASE#43125