Zynstra Technical Advisory

ZYN2015-06-001

Advisory Type	Security
Initial Release Date	01/06/2015
Version	1.0 (Initial Release)
Scope	First addressed in Zynstra releases 2.5.1 and 2.6.1

Executive Summary

Zynstra has deployed a Microsoft security update (KB3000483) that might require extra manual configuration steps by partners and/or end customers to fully protect against the Microsoft security vulnerability (MS15-011) that it addresses.

Description

Earlier this year, Microsoft issued a critical Windows security patch (KB3000483) that addresses a vulnerability in Group Policy processing. This patch, following the standard Zynstra patch testing process, has been tested as a bundle for stability and functionality alongside other 3rd party security patches and general updates on Zynstra's reference environments. Following this process, it has already been deployed as part of Zynstra's on-going keep current patching process to all Zynstra Appliances.

The reason for this advisory is that unlike the vast majority of 3rd party security patches, this patch potentially requires some manual configuration steps to be carried out after the patch has been deployed to provide complete protection against the security vulnerability that it addresses – it essentially provides additional security hardening capabilities that need to be enabled. Furthermore, some decisions need to be made in terms of the level, if any, of the security hardening applied in each environment and there are also some dependencies and interactions in terms of client PC versions (including other required updates for older Windows clients if the hardening is applied fully). Finally, it is also worth pointing out that to exploit the vulnerability this patch addresses, an attacker needs to first convince a user with a domain-configured system to connect to an attacker-controlled network and/or attacker-controlled servers AND for there to be scripts that are configured to run as part of one or more Group Policy Objects (GPOs).

Given this, Zynstra would like to highlight this to partners for them to consider the implications, and determine what manual configuration and security hardening, if any, to apply to each particular end customer environment. Full details of the vulnerability and the configuration steps are detailed here: https://support.microsoft.com/en-us/kb/3000483 and Zynstra recommends that partners read that article carefully in conjunction with this advisory.

Support

If you have any further questions, please contact Zynstra Customer Care as usual:

Phone

UK 0333 355 7054
(from within the UK)
+44 1225 388694
(from outside the UK)
US 1-877-410-7045

Email

support @ zynstra.com

support-**uk** @ zynstra.com

support-**us** @ zynstra.com

support-**de** @ zynstra.com

support-**nl** @ zynstra.com

support-**fr** @ zynstra.com

Internet

support.zynstra.com