Zynstra Technical Advisory

ZYN2017-08-001

Advisory Type	Security
Initial Release Date	07/08/2017
Author	Hakan Aysan
Version	1.0
Scope	First addressed in releases Jaguar 2060 and Llama 2.1.3

Executive Summary

Zynstra has deployed a Windows security update first included in the July Microsoft rollup updates (KB4025336 – Monthly Rollup and KB4025333 – Security-only update), and also included in future monthly roll-ups, that might require extra manual configuration steps by partners and/or end customers to fully protect against the security vulnerability (CVE-2017-8563) that it addresses.

Description

In July, Microsoft issued an important Windows security update (KB4025336/KB4025333 for Windows 2012R2) for multiple editions and versions of Windows, both client and server, that extends Extended Protection for Authentication for the LDAP protocol to protect against an elevation of privilege vulnerability through a man-in-the-middle attack. This update, following the standard Zynstra update 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 (including setting the LdapEnforceChannelBinding registry key) 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) as well as the timing of when the hardening is applied to other clients, servers and in particular other domain controllers not on the Zynstra server. Finally, it is also worth pointing out that to exploit the vulnerability this patch addresses, an attacker needs to already have the network access to intercept and forward authentication requests to a domain controller.

Given this, Zynstra would like to highlight this to partners and end customers and for them to consider the implications, and determine what manual configuration and security hardening, if any, to apply to their particular environment. Full details of the vulnerability and the configuration steps are detailed here: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8563 and here: https://support.microsoft.com/en-us/help/4034879/how-to-add-the-ldapenforcechannelbinding-registry-entry and Zynstra recommends that end customers and partners read that article carefully in conjunction with this advisory. Once the end customer and/or partner have determined the timing and values of any settings that need to be changed, they should raise a support ticket with Customer Care in the normal way for Zynstra to apply the changes to curated VMs running on the Zynstra platform.

Support

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

https://support.zynstra.com/hc/en-us/articles/201218972-How-do-I-contact-Zynstra-