11 May 2021

Attention To: Mr. Jeruel Sanz
EDP Manager
ENZI CORPORATION

Mr. Mark Nacionales
IT Specialist
ENZI CORPORATION

Subject: Penetration Test Report for Enzi Network

Dear Sirs:

Below is a list of opened and established ports with findings and recommendation per server checked in the ENZI Network as of May 11, 2021.

Server / IP	Port	Findings and Recommendation
Domain Controller	- Local Security Authentication Server - Service Host Process - WinVNC (Redundant) - AnyDesk - Microsoft Active Directory WebServices - Microsoft Spooler Subsystem - Domain Name System - Distributed File System Replication - Intersite Messaging Service - Microsoft Management Console - Dell DFS Service WinService	Uninstall Anydesk and WinVNC. Remove unattended access. Run only a portable version of remote access. All remote access must be monitored by IT. No other potential security vulnerability ports found. All services using ports are safe.
E-Mail Server	- Mail Server - HTTP - Service Host Process - System - Openfire as Service - Application Layer Gateway - MySQL - Symantec Antivirus - Local Security Authentication Server	No potential security vulnerability ports found. All services using ports are safe.
Enzi CRM Server	- System - Service Host Process - MSSQL Server - MSSQL Browser - Filezilla Server - Anydesk - Microsoft Spooler Subsystem - Windows Management Instrumentation Provider Service	Uninstall Anydesk and WinVNC. Remove unattended access. Run only a portable version of remote access. All remote access must be monitored by IT. FTP thru Filezilla is now the way to transfer files from clients to server and vice versa. No other potential security vulnerability ports found. All services using ports are safe.

File Server	- System - Service Host Process - Anydesk - Local Security Authentication Server - File Sharing	Uninstall Anydesk and WinVNC. Remove unattended access. Run only a portable version of remote access. All remote access must be monitored by IT. No potential security vulnerability ports found. All services using ports are safe.
Jeonsoft	- Filezilla - Free FTP Service (Redundant) - Service Host Process - WinVNC (Redundant) - Teamviewer - Microsoft SQL Server Analysis Services - Windows Start-Up Application - Local Security Authentication Server - JPS.exe (SUSPICIOUS - DANGEROUS unless Jeonsoft Program)	Uninstall Filezilla if not needed. Uninstall FTP Service if not needed Uninstall Teamviewer and WinVNC. Remove unattended access. Run only a portable version of remote access. All remote access must be monitored by IT. Ask Jeonsoft provider if JPS.exe is an executable from Jeonsoft
Quickbooks	- Service Host Process - WinVNC - Anydesk (Redundant) - Quickbooks - Putty Agent (Dangerous unless required by Quickbooks) - Windows Start-Up Application - Local Security Authentication Server - Microsoft Service and App Controller - Symantec Antivirus - CNAB3RPK.EXE - Canon Printer Free Fixer (SUSPICIOUS - Uninstall if not in use) - CNAB4RPK.EXE - Canon Printer Free Fixer (SUSPICIOUS - Uninstall if not in use) - Quickbooks Component	Uninstall PUTTY if not needed. Uninstall Anydesk. Remove unattended access. Run only a portable version of remote access. All remote access must be monitored by IT. Uninstall Canon Printer Free Fixer if not needed. CNAB3RPK.exe and CNAB3RPK.exe are potentially dangerous files downloaded from internet.
Text Commander	- Service Host Process - Anydesk - Local Security Authentication Server - Firefox (Close program when not in use)	Uninstall Anydesk. Remove unattended access. Run only a portable version of remote access. All remote access must be monitored by IT. Close all windows when not in use, i.e. Firefox

Voice Logger 1	**- Service Host Process - Local Security Authentication Server - Windows Start-Up Application - Recorder.exe - proPopup.exe - (SUSPICIOUS - Uninstall if not in use)**	**proPopup.exe is suspicious. Investigate if it's in the same folder of Recorder.exe**
Voice Logger 2	- Service Host Process - Local Security Authentication Server - Windows Start-Up Application - Recorder.exe - proPopup.exe - (SUSPICIOUS - Uninstall if not in use)	proPopup.exe is suspicious. Investigate if it's in the same folder of Recorder.exe
FIREWALL		Preliminary tests show that users can download TOR Browser. TOR Browser acts likes a VPN and can bypass security filters. Make sure to blacklist the tor browser site: Blacklist https://www.torproject.org

Test Performed and Analyzed by:

12 May 2021

Everett Gaius S. Vergara
Chief Technology Officer
FYDesigns, Inc.

Date