Good afternoon Jeremy and please read this critical notification in full.

Despite Microsoft's assertion that their latest update fixed last month's PrintNightmare vulnerabilities, we've been informed that additional critical security issues remain that we wanted to bring to your attention.

Although the recent patch resolved the original remote vulnerability issues, it does not address locally exploitable vulnerabilities. These local vulnerabilities can be exploited by anyone who is logged into the machine- including non-admin users- to gain full control of that device. If your workstation is unknowingly infected with malware it may present a considerable risk to your organization. **Unfortunately no fix from Microsoft has been identified, so they highly recommend to keep Print Spoolers disabled for the time being.** In the meantime, please discourage any users from bypassing these security measures and as an additional precaution, ensure that all users have rebooted their machines so that any critical anti-virus or security updates can be applied. TSI will notify you when Microsoft develops a fix for the most recent vulnerability.

Once you've reviewed this critical security update, please contact your account manager if you have any questions or concerns. Thank you in advance for your time and attention to this matter.

Sincerely,

Chris Souza

CMMC Registered Provider Organization

Technical Support INTERNATIONAL

Phone: (508) 543-6979 x119 | Fax: (508) 546-0252
Website | LinkedIn | Facebook | Twitter

Microsoft Partner
Gold Midmarket Solution Provider