Audience: All Interagency Incident Management Team CTSP personnel

From: Interagency Fire Community Technical

Date: 02 June 2015

HANDLING: Controlled Unclassified Information/Sensitive Security

Subject: NEW Forest Service AD Machine Group Policy that does not allow local drive mapping in support of United States Government Configuration Baseline minimum computer security settings

BLUF: Obtain Forest Service Local Drive Mapping tool from the Interagency Fire Helpdesk at 1-866-224-7677 in order to initiate waiver of policy patch on Forest Service laptops and/or desktops to ensure local drive mapping capability.

Background—

In order to remediate a material security finding against the Forest Service Network, a security change will be implemented on all Forest Service laptops and desktops that may impact local drive mapping to NAS devices. This security change may impact Incident Management Team’s with older NAS devices. If your team NAS device does not meet the minimum SAMBA level required by the security changes being pushed to Forest Service Laptops and Desktops, you may encounter errors when trying to map a local drive.

Resolution—

A patch has been made available that uses PowerBroker, the Forest Service’s Group Policy restriction-easement tool. This patch is available to any interagency CTSP at the Forest Service Interagency Fire Help Desk at 1-866-224-7677. This tool is intended to allow Forest Service users on assignment at the fire camp to map a local drive to a legacy NAS device. Once the tool is run on a Forest Service device the user will be able to map to a legacy NAS device while at the incident. The next time a user connects to the Forest Service Enterprise Network, either directly or through a VPN connection, the security change will be reapplied and the tool will need to be run again.

Technical Specifications—

Forest Service users with a Forest Service device will be unable to connect to a NAS with a version of SAMBA that is lower than 3.6. If your Incident Management Team NAS device operates with a version of SAMBA above 3.6 you will not need to run this tool as the Forest Service device can be mapped to the local drive. Prior to mobilization or upon arrival to your first incident this season please verify the SAMBA version of your IMT NAS device to determine the need for your team CTSP to run this tool on impacted devices.

1. If you receive the following error while trying to map a local drive from a forest service computer at your Incident Command Post *“The mapped network drive could not be created because the following error has occurred—The specified server cannot perform the requested operation”*
2. Call the Interagency HelpDesk to obtain the ***ReverseServerDriveMappingSettings.exe*** patch
3. Copy the patch to the user’s desktop
4. Run the patch (You do not need to run elevated or with an administrator account)
5. Restart the laptop/desktop
6. Attempt to map the drive again

Security Note and Recommendation—

The intent of the applied Group Policy is to eliminate the ability of a virus, threatware or malware from propagating through the local network. Some varieties of ransomware, malware and viruses spread through local drive mapping.

The older NAS devices that are affected by this Group Policy should be nearing end-of-life. New NAS devices that have current software should be procured to ensure IMT networks are not at risk. Having an up-to-date NAS operating system will reduce the risk to the incident network. Replacement of a team’s legacy NAS device may be a subject for pre-incident planning consideration. If a decision is made to acquire one, follow individual agency acquisition rules, or already-established incident management team procedures.