gluware®
Intelligent Network
Automation

Executive Brief

# Using Network Automation to Address Cybersecurity Threats

*By Mike Haugh, Gluware VP of Product Marketing, CCIE #4334 and Terry Slattery, Principal Architect at NetCraftsmen, CCIE #1026*

## Gluware® Intelligent Network Automation

Gluware is the recipient of the prestigious TechTarget **Network Innovation Award** for its innovative approach to intelligent multi-vendor, multi-domain, and multi-cloud network automation.

The widespread impact of the SolarWinds (Sunburst and Supernova) security hacks sent network teams scrambling to react, assess the impact, and mitigate any potential damage. Organizations needed to conduct a forensic assessment phase to determine if they were affected then follow the Cybersecurity and Infrastructure Security Agency (CISA) emergency directive 21-01 to take steps to address a possible breach.

*For more context on the breach check out this blog post from Gluware partner NetCraftsmen: An Executive's Guide to the Attack on FireEye and SolarWinds.*

CISA has released an alert (CISA Alert AA20-352A) that recommends mitigation steps to take for SolarWinds Orion and to address potential vulnerabilities left in the network infrastructure by the threat actors. Organizations that have network automation in place are equipped to automate many of the CISA recommended mitigation actions for all network devices (router, switches, firewalls, etc.). The Gluware® Intelligent Network Automation software solution can aid an organization in quickly implementing these actions.

## CISA Recommendation: Device configurations

- Audit all network device configurations, stored or managed on the SolarWinds monitoring server, for signs of unauthorized or malicious configuration changes.
- Audit the configurations found on network devices for signs of unauthorized or malicious configuration changes. Organizations should ensure they audit the current network device running configuration and any local configurations that could be loaded at boot time.

### How Gluware Helps

- Use the Config Drift & Audit app to run a daily drift analysis and understand exactly what changes are being made on every network device configuration. We also recommend integrating Syslog so there is correlation with the user credentials that were used to make the change.
- Use the Config Drift & Audit app to run regular company policy audits to ensure the configurations remain compliant with an organization's network configuration policies (on a per-feature basis). This is particularly important for network system security policies and firewall rules.
- Use the Device Manager app to provide visibility on the operating system version running and the "up time" for an indicator if a device was potentially rebooted.

## CISA Recommendation: Credential and security information reset

Change all credentials being used to manage network devices, to include keys and strings used to secure network device functions (SNMP strings/user credentials, IPsec/IKE pre-shared keys, routing secrets, TACACS/RADIUS secrets, RSA keys/certificates, etc.)

### How Gluware Helps

Use the Config Modeling app to automate (at a minimum) the configuration policies. Gluware Config Modeling provides an intent-based, declarative method to intelligently automate any network configuration (feature by feature). Users can define their own policy (intended state) and The Gluware engine will implement the changes to the network layer reliably and at scale. It is also able to remove old/incorrect policies instead of just adding more and increasing the technical debt. In this example, Config Modeling can be used for:

- Authentication, including any TACACS/RADIUS/AAA configuration.
- Automate your SNMP policies and use Gluware to make any changes if removing access to the SolarWinds servers and changing SNMP servers.
- Automate your Syslog policy and ensure every device is configured for the proper logging servers. CISA recommends storing logs for 180 days.
- Automate and reset any static user credentials on each device.
- Verify your routing policies (and any related ACLs) to ensure they have not been tampered with and remediate if necessary.
- Use Gluware to automate the deployment of new pre-shared keys and to update certificates

## CISA Recommendation: Firmware and software validation

Validate all network device firmware/software which was stored or managed on the SolarWinds monitoring server. Cryptographic hash verification should be performed on such firmware/software and matched against known good hash values from the network vendor. CISA recommends that, if possible, organizations download known good versions of firmware.

### How Gluware Helps

- Use the OS Manager app to automate any upgrades/downgrades/patches which integrates a validation of the checksum (it can automate the check for Cisco device operating systems using Gluware's API integration).
- Use Device Manager to closely monitor the deployed versions of OSes running in your network. We strongly recommend tracking security vulnerabilities against all versions of network equipment operating systems. Apply patches and workarounds as needed to prevent future cyber-attacks.

These are just a few examples of how having network automation in place will help organizations assess and take action to mitigate any risk to their network and in turn protect their infrastructure and data. The above recommendations from CISA, while specific to a specific cybersecurity threat, are actually best practices that should be part of any IT security system.

References: https://www.solarwinds.com/securityadvisory/faq | https://us-cert.cisa.gov/ncas/alerts/aa20-352a