Hardening Networked Systems for Local Government & Critical Infrastructure

Threat Level: HIGH

Overview: Recent high-profile cyber incidents affecting Mississippi's critical infrastructure underscore a persistent and evolving threat landscape. Threat actors are increasingly utilizing unauthenticated remote code execution (RCE) and sophisticated social engineering to paralyze essential services.

In light of these events, the Mississippi Cyber Unit (MCU) recommends that all local government and critical infrastructure entities immediately adopt a "Defend Forward" posture.

Critical Threat Vectors & Observations:

1. **Appliance Vulnerabilities:** Recent exploitation of edge devices (e.g., Ivanti EPMM CVE-2026-1281, BeyondTrust CVE-2026-1731, Fortinet CVE-2026-24858) has shown that attackers are targeting the "keys to the kingdom." Unpatched remote access tools are being used as entry points for SparkRAT and VShell backdoors.

2. **Data Exfiltration & Double Extortion:** Attackers are no longer just locking systems; they are exfiltrating sensitive data prior to encryption to maximize leverage.

3. **Lateral Movement:** Once initial access is gained, actors are utilizing specialized tools like *Impacket* and *Mimikatz* to move from administrative workstations to core server environments.

Critical Examples of Edge Exploitation

Recent intelligence indicates edge device vulnerabilities being weaponized to gain initial access and establish long-term persistence:

1. **Ivanti EPMM (CVE-2026-1281):** A critical pre-authentication Remote Code Execution (RCE) vulnerability. This flaw allows an unauthenticated attacker to execute arbitrary commands with system-level privileges through a maliciously crafted HTTP request. It specifically targets legacy Bash scripts used for URL rewriting.

2. **BeyondTrust (CVE-2026-1731):** A critical pre-authentication RCE vulnerability in Privileged Remote Access (PRA) and Remote Support appliances. Attackers utilize a crafted WebSocket message to trigger a command injection in the thin-scc-wrapper component, allowing for the deployment of backdoors like *SparkRAT* and *VShell*.

3. **Fortinet (CVE-2026-24858):** A high-severity authentication bypass in FortiOS and FortiProxy. This vulnerability allows an unauthenticated attacker to gain access to management interfaces, enabling the reconfiguration of firewall rules or the creation of unauthorized administrative accounts.

Operational Impact & Observed Tactics:

When edge devices are compromised, the impact on critical infrastructure is immediate:

- **Credential Harvesting:** Attackers gain direct access to stored passwords, SSH keys, and session tokens within credential vaults.
- **Lateral Movement:** Once the gateway is breached, actors utilize tools like *Impacket* to traverse from the perimeter to core servers and database environments.
- **Ransomware Positioning:** Access brokers are using these specific CVEs to sell "entry points" to ransomware affiliates, who then exfiltrate data for double-extortion campaigns.

Immediate Action Items:

1. Zero-Trust Access & Identity Management
   - *Enforce Phishing-Resistant MFA:* Transition all administrative access to hardware-based security keys (FIDO2/WebAuthn). Traditional SMS or push-based MFA is insufficient against actors targeting administrative session tokens.
   - *Account Auditing:* Conduct an immediate audit of all "Domain Admin" and "Enterprise Admin" groups for any unauthorized accounts created in the last 30 days.

2. Aggressive Patch Management
   - *Standardize Priority Patching for Edge Devices:* Any appliance exposed to the internet (VPNs, Load Balancers, Gateways) must be patched as soon as possible following the release of a critical CVE release.
   - *Legacy System Isolation:* Systems that cannot be patched (e.g., specialized medical or utility hardware) must be air-gapped or placed behind a strict stateful inspection firewall with zero outbound internet access.

3. Network Segmentation & Monitoring
   - *Micro-Segmentation:* Isolate critical data stores (SQL databases, patient records) from general office networks to prevent lateral movement.
   - *Endpoint Detection & Response (EDR):* Deploy EDR agents in "Block" mode on all management workstations and servers.
   - *Logging:* Ensure all appliance logs (especially WebSocket handshakes and HTTP GET requests to management endpoints) are forwarded to an immutable, centralized log management system for retroactive analysis.

Resources:

Information and links are all designated **Traffic Light Protocol (TLP) – CLEAR**. Recipients may share **TLP: CLEAR** information without restriction, information is subject to standard copyright rules. External links are not maintained by the MOHS. External links are provided for convenience and do not represent endorsement by MOHS or the Department of Public Safety (DPS) for any commercial or private issues, products, or services.

- Unit 42 (BeyondTrust CVE-2026-1731 Analysis)
- SentinelOne (Ivanti EPMM CVE-2026-1281 Analysis)
- Fidelis Security (Fortinet Auth Bypass CVE-2026-24858)
- CISA (Known Exploited Vulnerabilities Catalog)

Report Suspicious Activity

Citizens should always call local law enforcement first. Local government and critical infrastructure can report suspected cyberattacks, by contacting calling 601-933-7200, 1-888-4SAFE-MS or email ms-cyber@dps.ms.gov. Email is not monitored 24 hours a day, if there is an emergency, please dial 911.

(U) Standing Information Needs (SINS) Supported:

- HSEC-1.1: Cyber Attacks and Exploitation
- MS-14000-09: Cyber Crime