H E A D Q U A R T E R S
ARMED FORCES OF THE PHILIPPINES CYBER COMMAND
Camp General Emilio Aguinaldo, Quezon City

CYBERSECURITY BULLETIN 2025-06

Critical Windows Task Scheduler Vulnerability Enables Privilege Escalation

Overview

A newly discovered privilege escalation vulnerability in Microsoft Windows Task Scheduler, tracked as CVE-2025-33067, poses a critical risk to affected systems. The flaw allows local attackers to gain system-level access without requiring administrative privileges or user interaction. Microsoft released comprehensive security patches on June 10, 2025, and organizations are urged to deploy updates immediately.

Affected systems are Windows 10 (1607, 1809, 21H2, 22H2), Windows 11 (22H2, 23H2, 24H2) and Windows Server 2016 – 2025.

The vulnerability allows an attacker with local access, even without elevated rights to exploit improper permission handling in scheduled task components. If successful, they can escalate to the system and gain the highest privilege level in Windows, potentially bypassing endpoint security and gaining unrestricted control.

While no active exploitation has been observed, the nature of the vulnerability makes it a high-value target for threat actors seeking lateral movement or persistence within compromised environments.

Recommendations:

Following are the recommended actions to reduce exposure to the said vulnerability:

1. **Immediate Patch Deployment**
   - Prioritize patching high-value systems, legacy OS versions, and servers exposed to user activity or public access.

2. **Review and Harden Scheduled Tasks**
   - Audit all scheduled tasks for unauthorized access or misconfigurations.
   - Enforce access controls using the principle of least privilege.

3. **Implement Network Segmentation**
   - Limit lateral movement opportunities by isolating critical systems from general user workstations.

4. **Enhance Endpoint Monitoring**
   - Monitor for abnormal usage of Task Scheduler (schtasks.exe) or unusual creation/editing of scheduled tasks.

5. **Review Access Logs and System Events**
   - Examine system logs for recent privilege elevation or anomalous process execution activity related to task scheduling.

6. **Educate and Train Users**
   - Reinforce phishing awareness to reduce the chances of initial access, which attackers may leverage to exploit CVE-2025-33067.

Conclusion

CVE-2025-33067 demonstrates how a single local vulnerability can be leveraged for full system compromise. Even in the absence of public exploits, the low complexity and high impact of this flaw make it essential for organizations to patch quickly, reinforce access controls, and improve monitoring for privilege escalation attempts.

Stay alert. Stay protected.

Reference: https://cybersecuritynews.com/windows-task-scheduler-vulnerability/