Posted Date: 2025/11/18

[Vulnerability Alert] CISA Added 5 Known Exploited Vulnerabilities to KEV Catalog (2025/11/10-2025/11/16)

- Subject: [Vulnerability Alert] CISA Added 5 Known Exploited Vulnerabilities to KEV Catalog (2025/11/10-2025/11/16)
- Content:
  - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center Security Alert TWCERTCC-200-202511-00000012
  - - [CVE-2025-21042] Samsung Mobile Devices Out-of-Bounds Write Vulnerability (CVSS v3.1: 8.8)
  - [Exploited by Ransomware: Unknown] Samsung mobile devices have an Out-of-Bounds Write vulnerability in libimagecodec.quram.so. This vulnerability may allow a remote attacker to execute arbitrary code.
  - - [CVE-2025-12480] Gladinet Triofox Improper Access Control Vulnerability (CVSS v3.1: 9.1)
  - [Exploited by Ransomware: Unknown] Gladinet Triofox has an Improper Access Control vulnerability that allows access to the initial setup page even after configuration is complete.
  - - [CVE-2025-62215] Microsoft Windows Race Condition Vulnerability (CVSS v3.1: 7.0)
  - [Exploited by Ransomware: Unknown] Microsoft Windows kernel has a Race Condition vulnerability that allows a local attacker with low-level privileges to elevate privileges. Successful exploitation of this vulnerability may allow the attacker to gain SYSTEM-level access.
  - - [CVE-2025-9242] WatchGuard Firebox Out-of-Bounds Write Vulnerability (CVSS v3.1: 9.8)
  - [Exploited by Ransomware: Unknown] The iked process in the WatchGuard Firebox operating system has an Out-of-Bounds Write vulnerability, which may allow an unauthenticated remote attacker to execute arbitrary code.
  - - [CVE-2025-64446] Fortinet FortiWeb Path Traversal Vulnerability (CVSS v3.1: 9.8)
  - [Exploited by Ransomware: Unknown] Fortinet FortiWeb has a Path Traversal vulnerability, which may allow an unauthenticated attacker to execute administrative commands on the system through specially crafted HTTP or HTTPS requests.
- Affected Platforms:
  - [CVE-2025-21042] Please refer to the official listed affected versions https://security.samsungmobile.com/securityUpdate.smsb
  - [CVE-2025-12480] TrioFox versions up to and including 16.7.10368.56560
  - [CVE-2025-62215] Please refer to the official listed affected versions https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-62215
  - [CVE-2025-9242] Please refer to the official listed affected versions https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00015
  - [CVE-2025-64446] Please refer to the official listed affected versions https://fortiguard.fortinet.com/psirt/FG-IR-25-910
- Recommended Measures:
  - [CVE-2025-21042] The official source has released a fix update for the vulnerability;

please update to the relevant version https://security.samsungmobile.com/securityUpdate.smsb
- [CVE-2025-12480] Upgrade the corresponding product to TrioFox versions later than 16.7.10368.56560 (exclusive) (or higher)
- [CVE-2025-62215] The official source has released a fix update for the vulnerability; please update to the relevant version https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-62215
- [CVE-2025-9242] The official source has released a fix update for the vulnerability; please update to the relevant version https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00015
- [CVE-2025-64446] The official source has released a fix update for the vulnerability; please update to the relevant version https://fortiguard.fortinet.com/psirt/FG-IR-25-910

Computer and Communications Center
Network Systems Group