Date Posted: 2026/02/06

[Vulnerability Alert] CISA Adds 7 Known Exploited Vulnerabilities to KEV Catalog (2026/01/26-2026/02/01)

- Subject Explanation: [Vulnerability Alert] CISA Adds 7 Known Exploited Vulnerabilities to KEV Catalog (2026/01/26-2026/02/01)
- Content Description:
  - Forwarding Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) Security Alert TWCERTCC-200-202602-00000001
  - [CVE-2018-14634] Linux Kernel Integer Overflow Vulnerability (CVSS v3.1: 7.8)
  - [Ransomware Usage: Unknown] An integer overflow vulnerability exists in the create_elf_tables() function in the Linux Kernel, which may allow an unprivileged local user with access to SUID (or other privileged) binaries to escalate privileges.
  - [CVE-2025-52691] SmarterTools SmarterMail Unrestricted Upload of File with Dangerous Type Vulnerability (CVSS v3.1: 10.0)
  - [Ransomware Usage: Unknown] SmarterTools SmarterMail contains an unrestricted dangerous file type upload vulnerability, which may allow an unauthenticated attacker to upload arbitrary files to any location on the mail server, potentially leading to remote code execution.
  - [CVE-2026-23760] SmarterTools SmarterMail Authentication Bypass Using an Alternate Path or Channel Vulnerability (CVSS v3.1: 9.8)
  - [Ransomware Usage: Unknown] SmarterTools SmarterMail contains an authentication bypass vulnerability in the password reset API. The force-reset-password endpoint allows anonymous requests and fails to verify the existing password or reset token when resetting the administrator account. An unauthenticated attacker only needs to provide the target administrator username and a new password to reset the account, resulting in the takeover of the SmarterMail instance.
  - [CVE-2026-24061] GNU InetUtils Argument Injection Vulnerability (CVSS v3.1: 9.8)
  - [Ransomware Usage: Unknown] An argument injection vulnerability exists in telnetd of GNU InetUtils. Attackers can bypass remote authentication by setting the USER environment variable to “-f root”.
  - [CVE-2026-21509] Microsoft Office Security Feature Bypass Vulnerability (CVSS v3.1: 7.8)
  - [Ransomware Usage: Unknown] Microsoft Office contains a security feature bypass vulnerability. The vulnerability arises from its reliance on untrusted input during the security decision process, which may allow an unauthorized attacker to bypass security protection mechanisms locally. Some affected products may have reached End of Life (EoL) and/or End of Service (EoS). Users are advised to discontinue use and migrate to a supported version.
  - [CVE-2026-24858] Fortinet Multiple Products Authentication Bypass Using an Alternate Path or Channel Vulnerability (CVSS v3.1: 9.8)
  - [Ransomware Usage: Unknown] An authentication bypass vulnerability exists in Fortinet FortiAnalyzer, FortiManager, FortiOS, and FortiProxy. When FortiCloud SSO authentication is enabled on the affected device, an attacker with a FortiCloud account and a registered device may log into a device registered under another account.
  - [CVE-2026-1281] Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability

(CVSS v3.1: 9.8)
    - [Ransomware Usage: Unknown] Ivanti Endpoint Manager Mobile (EPMM) contains a code injection vulnerability that may allow an attacker to achieve remote code execution without authentication.
- Impacted Platforms:
    - [CVE-2018-14634]
    - Linux kernel versions 2.6.0 to 2.6.39.4
    - Linux kernel versions 3.10 to 3.10.102
    - Linux kernel versions 4.14 to 4.14.54
    - [CVE-2025-52691]
    - Versions prior to SmarterTools SmarterMail Build 9413
    - [CVE-2026-23760]
    - Versions prior to SmarterTools SmarterMail Build 9511
    - [CVE-2026-24061]
    - Please refer to the affected versions listed officially: https://lists.gnu.org/archive/html/bug-inetutils/2026-01/msg00004.html
    - [CVE-2026-21509]
    - Please refer to the affected versions listed officially: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509
    - [CVE-2026-24858]
    - Please refer to the affected versions listed officially: https://fortiguard.fortinet.com/psirt/FG-IR-26-060
    - [CVE-2026-1281]
    - Please refer to the affected versions listed officially: https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340
- Suggested Measures:
    - [CVE-2018-14634]
    - System administrators should check with their product vendor to see if their Linux operating system is affected. If a patch is available, follow the vendor's recommendations and take immediate action to reduce risk.
    - [CVE-2025-52691]
    - Upgrade the corresponding product to the following version (or higher): SmarterMail Build 9413
    - [CVE-2026-23760]
    - Upgrade the corresponding product to the following version (or higher): SmarterMail Build 9511
    - [CVE-2026-24061]
    - The official vendor has released a repair update for the vulnerability; please update to the relevant version: https://lists.gnu.org/archive/html/bug-inetutils/2026-01/msg00004.html
    - [CVE-2026-21509]
    - The official vendor has released a repair update for the vulnerability; please update to the relevant version: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509
    - [CVE-2026-24858]
    - The official vendor has released a repair update for the vulnerability; please update to the relevant version: https://fortiguard.fortinet.com/psirt/FG-IR-26-060
    - [CVE-2026-1281]
    - The official vendor has released a repair update for the vulnerability; please update to the relevant version: https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPM

M-CVE-2026-1281-CVE-2026-1340

Computer and Communication Center Network Systems Division