Date Posted: 2025/07/16

□Vulnerability Alert□CISA Adds 5 Known Exploited Vulnerabilities to KEV Catalog (2025/07/07-2025/07/13)

- Subject: □Vulnerability Alert□CISA Adds 5 Known Exploited Vulnerabilities to KEV Catalog (2025/07/07-2025/07/13)
- Content Description:
    - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center TWCERTCC-200-202507-00000010
    1. [cite_start]□CVE-2019-9621□Synacor Zimbra Collaboration Suite (ZCS) Server-Side Request Forgery (SSRF) Vulnerability (CVSS v3.1: 7.5) [cite: 4]
        - [cite_start]□Exploited by Ransomware: Unknown□ Synacor Zimbra Collaboration Suite has a Server-Side Request Forgery vulnerability through the ProxyServlet component. [cite: 4]
        - [cite_start]□Affected Platforms□Please refer to the affected versions listed on the official website [cite: 4]
        - [cite_start]https://blog.zimbra.com/2019/05/9826/ [cite: 4]
    2. [cite_start]□CVE-2019-5418□Rails Ruby on Rails Path Traversal Vulnerability (CVSS v3.1: 7.5) [cite: 4]
        - [cite_start]□Exploited by Ransomware: Unknown□ Rails Ruby on Rails has a path traversal vulnerability in Action View. [cite: 4] [cite_start]Combined with a specially crafted Accept header and a call to render file:, this could lead to the leakage of arbitrary file contents on the target server. [cite: 4]
        - [cite_start]□Affected Platforms□Please refer to the affected versions listed on the official website [cite: 4]
        - [cite_start]https://web.archive.org/web/20190313201629/https://weblog.rubyonrails.org/2019/3/13/Rails-4-2-5-1-5-1-6-2-have-been-released/ [cite: 4]
    3. [cite_start]□CVE-2016-10033□PHPMailer Command Injection Vulnerability (CVSS v3.1: 9.8) [cite: 4]
        - [cite_start]□Exploited by Ransomware: Unknown□ PHPMailer has a command injection vulnerability due to improper handling of user-provided input. [cite: 4] [cite_start]Attackers can exploit this vulnerability to execute arbitrary code within the context of the application, and failed attack attempts may lead to denial of service. [cite: 4]
        - [cite_start]□Affected Platforms□Please refer to the affected versions listed on the official website [cite: 4]
        - [cite_start]https://github.com/PHPMailer/PHPMailer/wiki/About-the-CVE-2016-10033-and-CVE-2016-10045-vulnerabilities [cite: 4]
    4. [cite_start]□CVE-2014-3931□Multi-Router Looking Glass (MRLG) Buffer Overflow Vulnerability (CVSS v3.1: 9.8) [cite: 4]
        - [cite_start]□Exploited by Ransomware: Unknown□ Multi-Router Looking Glass has a buffer overflow vulnerability, which can lead to arbitrary memory writes and memory corruption by remote attackers. [cite: 4]
        - [cite_start]□Affected Platforms□Please refer to the affected versions listed on the official website [cite: 4]

    - [cite_start]https://mrlg.op-sec.us/ [cite: 4]

5. [cite_start]□CVE-2025-5777□Citrix NetScaler ADC and Gateway Out-of-Bounds Read Vulnerability (CVSS v3.1: 7.5) [cite: 5]
    - [cite_start]□Exploited by Ransomware: Unknown□ Citrix NetScaler ADC and Gateway have an out-of-bounds read vulnerability due to insufficient input validation. [cite: 5] [cite_start]When NetScaler is configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) or AAA virtual server, this vulnerability may lead to memory over-read. [cite: 5]
    - [cite_start]□Affected Platforms□Please refer to the affected versions listed on the official website [cite: 5]
    - [cite_start]https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX693420 [cite: 5]

Computer and Communications Center
Network Systems Division Respectfully