Date Posted: 2025/07/02

□Vulnerability Alert□CISA Adds 3 Known Exploited Vulnerabilities to KEV Catalog (2025/06/23-2025/06/29)

- Subject: □Vulnerability Alert□CISA Adds 3 Known Exploited Vulnerabilities to KEV Catalog (2025/06/23-2025/06/29)
- Content Description:
  - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center TWCERTCC-200-202507-00000001
  1. □CVE-2019-6693□Fortinet FortiOS Use of Hard-Coded Credentials Vulnerability (CVSS v3.1: 6.5)
     - □Exploited by Ransomware: Unknown□ Fortinet FortiOS has a hard-coded credentials vulnerability, allowing attackers to encrypt and decrypt sensitive data in FortiOS configuration backup files using known hard-coded keys.
     - □Affected Platforms□ Please refer to the officially listed affected versions
     - https://fortiguard.fortinet.com/psirt/FG-IR-19-007
  2. □CVE-2024-0769□D-Link DIR-859 Router Path Traversal Vulnerability (CVSS v3.1: 9.8)
     - □Exploited by Ransomware: Unknown□ The D-Link DIR-859 router has a path traversal vulnerability in the /hedwig.cgi file within its HTTP POST request handling component, which could lead to privilege escalation and unauthorized device control.
     - □Affected Platforms□ Please refer to the officially listed affected versions
     - https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10371
  3. □CVE-2024-54085□AMI MegaRAC SPx Authentication Bypass by Spoofing Vulnerability (CVSS v3.1: 9.8)
     - □Exploited by Ransomware: Unknown□ AMI MegaRAC SPx has an authentication bypass vulnerability through spoofing in the Redfish host interface. Successful exploitation of this vulnerability could lead to loss of confidentiality, integrity, and/or availability.
     - □Affected Platforms□ Please refer to the officially listed affected versions
     - https://www.ami.com/security-center/
- Affected Platforms:
  - Detailed content in the affected platforms section of the content description
- Suggested Measures:
  1. □CVE-2019-6693□ Official patches have been released for the vulnerability, please update to the relevant versions
     - https://fortiguard.fortinet.com/psirt/FG-IR-19-007
  2. □CVE-2024-0769□ Affected products may have reached End of Life (EoL) and/or End of Service (EoS). Users are advised to stop using these products.
  3. □CVE-2024-54085□ Official patches have been released for the vulnerability, please update to the relevant versions
     - https://www.ami.com/security-center/

Computer and Communications Center
Network Systems Division Respectfully