مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in Arcserve Unified Data Protection (UDP)

Tracking #:432315707

Date:18-03-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Multiple Vulnerabilities in Arcserve Unified Data Protection (UDP) that could be exploited to gain unauthorized access to affected systems.

TECHNICAL DETAILS:

Three critical vulnerabilities have been identified in Arcserve UDP Console that can be exploited by attackers to compromise affected systems. An attacker can potentially gain unauthorized access, upload malicious files, and crash the software.

- **CVE-2024-0799:** (CVSS Score: 9.8 CRITICAL) Authentication Bypass Vulnerability
- **CVE-2024-0800:** (CVSS Score: 8.8 HIGH) Path Traversal Vulnerability
- **CVE-2024-0801:** (CVSS Score: 7.5. HIGH) Unauthenticated Denial-of-Service (DoS) Vulnerability

These vulnerabilities can be chained together to achieve a more severe attack. A successful exploit could allow attackers to take complete control of the affected system.

- Proof-of-concept (PoC) exploit code is publicly available

Fixed Versions:

- Arcserve UDP 8.1-Patch P00003059
- Arcserve UDP 9.2-Patch P00003050

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by Arcserve.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

https://www.tenable.com/security/research/tra-2024-07
https://support.arcserve.com/s/article/P00003059?language=en_US
https://support.arcserve.com/s/article/P00003050?language=en_US