مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical Zero-Day Vulnerability in ScienceLogic EM7

Tracking #:432316422

Date:22-10-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical zero-day vulnerability discovered in the ScienceLogic EM7 (SL1) monitoring platform that allows for remote code execution.

TECHNICAL DETAILS:

CVE-2024-9537 is a critical zero-day vulnerability discovered in the ScienceLogic EM7 (SL1) monitoring platform, classified with a CVSS score of 9.8. This vulnerability allows for remote code execution, posing significant risks to organizations utilizing this software. Rackspace breach incident was notably linked to exploitation this flaw, where unauthorized access to performance monitoring data occurred.

Incident Background:

- On September 24, 2024, Rackspace identified suspicious activity linked to a zero-day vulnerability in a third-party utility bundled with ScienceLogic EM7. The investigation revealed that an unknown threat actor exploited this vulnerability, gaining access to performance monitoring data, including customer account names and device IDs, though no sensitive financial information was compromised.

Impact Assessment:

- The exploitation allowed unauthorized access to three internal monitoring web servers at Rackspace but did not disrupt customer performance monitoring services. The breach was confined to less sensitive data, yet it underscores the critical nature of patching vulnerabilities promptly.

Mitigation Efforts:

- Following the discovery, Rackspace collaborated with ScienceLogic to develop and deploy a patch for affected versions of SL1. CISA has added CVE-2024-9537 to its Known Exploited Vulnerabilities Catalog, urging immediate action from organizations using the affected software.

Patched Versions:

- 12.1.3+, 12.2.3+, and 12.3+

RECOMMENDATIONS:

The UAE Cyber Security Council recommends Organizations using ScienceLogic SL1 should upgrade to the latest versions immediately to mitigate the risk.

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.cve.org/CVERecord?id=CVE-2024-9537