مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Sandbox Escape Vulnerabilities in Judge0

Tracking #:432315806

Date:01-05-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Multiple critical vulnerabilities in Judge0, an open-source online code execution platform. These vulnerabilities could allow attackers with sufficient access to completely take over affected systems.

TECHNICAL DETAILS:

Vulnerabilities Details:

- **CVE-2024-28185 (CVSS: 10.0):** Improper handling of symlinks within the sandbox allows attackers to write to arbitrary files and execute code outside the sandbox.
- **CVE-2024-28189 (CVSS: 10.0):** Patch bypass for CVE-2024-28185. Attackers can leverage symlinks to gain unauthorized code execution outside the sandbox.
- **CVE-2024-29021 (CVSS: 9.1):** Improper configuration allows Server-Side Request Forgery (SSRF) attacks. Attackers can exploit this to gain full root access on the system.

Impact:

An attacker exploiting these vulnerabilities could gain complete control over the affected system, including access to the database, internal networks, web server, and potentially other applications running on the host machine.

Affected Products:

- Judge0 versions prior to 1.13.1

Fixed Versions:

- Judge0 to version 1.13.1 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Vendor.

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://github.com/judge0/judge0/security/advisories/GHSA-h9g2-45c8-89cf
- https://github.com/judge0/judge0/security/advisories/GHSA-3xpw-36v7-2cmg
- https://github.com/judge0/judge0/security/advisories/GHSA-q7vg-26pg-v5hr