مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in Ivanti Endpoint Manager (EPM)

Tracking #:432315901

Date:29-05-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in Ivanti Endpoint Manager (EPM) that could be exploited to gain unauthorized access to affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-22058**
- CVSS Score 7.8 High
- A vulnerability exists in Ivanti Endpoint Manager (EPM) that allows a local attacker with low privileges to escalate their privileges to administrator level. This vulnerability affects the legacy Remote Control functionality.
- A buffer overflow vulnerability allows a low privileged user on a machine with the EPM Agent installed to execute arbitrary code with elevated permissions within Ivanti EPM.
- A successful exploit of this vulnerability could allow an attacker to gain complete control over a vulnerable system. This could lead to data theft, deployment of malware, disruption of critical systems, or other malicious activities.

Affected Versions:

- Ivanti Endpoint Manager (EPM) versions 2021.1 SU5 and earlier

Fixed Versions:

- Ivanti Endpoint Manager (EPM) Version 2022 or later

RECOMMENDATIONS:

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

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://forums.ivanti.com/s/article/CVE-2024-22058-Privilege-Escalation-for-Ivanti-Endpoint-Manager-EPM?language=en_US