



مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**Security Updates-Ivanti Products**

Tracking #:432315719

Date:21-03-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Ivanti has released security updates to address several vulnerabilities in its products.

## TECHNICAL DETAILS:

### Vulnerabilities Details:

#### 1. Ivanti Neurons for ITSM:

- CVE-2023-4680
- A patch is now available for all supported versions of Ivanti Neurons for ITSM (2023.3, 2023.2 and 2023.1), and the patch has been applied to all Ivanti Neurons for ITSM Cloud landscapes.
- Unsupported versions are also at risk, customers should upgrade to a supported version before applying the patch.

#### 2. Ivanti Standalone Sentry:

- CVE-2023-41724- Critical RCE vulnerability
- The vulnerability affects all supported version of Ivanti Standalone Sentry (9.17.0, 9.18.0, and 9.19.0) as well as older, unsupported ones (<9.17.0).
- Users of the latter are advised to upgrade to a supported version and deploy the patch (9.17.1, 9.18.1 or 9.19.1).

## 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:

1. <https://www.ivanti.com/blog/security-update-for-ivanti-standalone-sentry>
2. <https://www.ivanti.com/blog/security-update-for-ivanti-neurons-for-itsm>