مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates-Ivanti Products

Tracking #:432315880

Date:22-05-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Ivanti released security updates to address multiple vulnerabilities in the Ivanti products.

TECHNICAL DETAILS:

On May 21, 2024 Ivanti released security bulletin addresses critical and high-severity vulnerabilities discovered in various Ivanti products.

Vulnerabilities addressed:

Ivanti Avalanche		
CVE	Description	CVSS
CVE-2024-29848	An unrestricted file upload vulnerability in web component of Ivanti Avalanche before 6.4.x allows an authenticated, privileged user to execute arbitrary commands as SYSTEM.	7.2
Ivanti Neurons for ITSM		
CVE	Description	CVSS
CVE-2024-22059	A SQL injection vulnerability in web component of Ivanti Neurons for ITSM allows a remote authenticated user to read/modify/delete information in the underlying database. This may also lead to DoS.	8.8
CVE-2024-22060	An unrestricted file upload vulnerability in web component of Ivanti Neurons for ITSM allows a remote, authenticated, high privileged user to write arbitrary files into sensitive directories of ITSM server.	8.7
Ivanti Connect Secure		
CVE	Description	CVSS
CVE-2023-38551	A CRLF Injection vulnerability in Ivanti Connect Secure (9.x, 22.x) allows an authenticated high-privileged user to inject malicious code on a victim's browser, thereby leading to cross-site scripting attack.	8.2
Ivanti Secure Access		
CVE	Description	CVSS
CVE-2023-38042	A local privilege escalation vulnerability in Ivanti Secure Access Client for Windows allows a low privileged user to execute code as SYSTEM.	7.8
CVE-2023-46810	A local privilege escalation vulnerability in Ivanti Secure Access Client for Windows allows a low privileged user to execute code as SYSTEM.	7.3
Ivanti Endpoint Manager (EPM)		
CVE	Description	CVSS
CVE-2024-29822	An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2022 SU5 and prior allows an unauthenticated attacker within the same network to execute arbitrary code.	9.6

CVE-2024-29823	An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2022 SU5 and prior allows an unauthenticated attacker within the same network to execute arbitrary code.	9.6
CVE-2024-29824	An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2022 SU5 and prior allows an unauthenticated attacker within the same network to execute arbitrary code.	9.6
CVE-2024-29825	An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2022 SU5 and prior allows an unauthenticated attacker within the same network to execute arbitrary code.	9.6
CVE-2024-29826	An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2022 SU5 and prior allows an unauthenticated attacker within the same network to execute arbitrary code.	9.6
CVE-2024-29827	An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2022 SU5 and prior allows an unauthenticated attacker within the same network to execute arbitrary code.	9.6
CVE-2024-29828	An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2022 SU5 and prior allows an authenticated attacker within the same network to execute arbitrary code.	8.4
CVE-2024-29829	An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2022 SU5 and prior allows an authenticated attacker within the same network to execute arbitrary code.	8.4
CVE-2024-29830	An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2022 SU5 and prior allows an authenticated attacker within the same network to execute arbitrary code.	8.4
CVE-2024-29846	An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2022 SU5 and prior allows an authenticated attacker within the same network to execute arbitrary code.	8.4

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to apply the security patch as soon as possible.

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/Security-Advisory-May-2024?language=en_US