مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in Ivanti Avalanche

Tracking #:432315769

Date:18-04-2024

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 INTELLGIENCE 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 that Ivanti recently released security updates to patch multiple vulnerabilities in Avalanche.

TECHNICAL DETAILS:

Ivanti has released a new product update for its flagship Avalanche mobile device management (MDM) product to fix 27 vulnerabilities, including two critical bugs. The remaining 25 CVEs fixed in this update are mainly path traversal and out-of-bounds read flaws with CVSS scores ranging from 5.3 to 8.8.

The critical flaws could lead to remote code execution (RCE). Ivanti stated that it was not aware of any of the vulnerabilities being actively exploited in the wild.

The two critical vulnerabilities are stack-based buffer overflow RCE and heap-based buffer overflow RCE, which can be exploited by unauthenticated attackers in low-complexity attacks without requiring user interaction

1. **CVE-2024-29204-CVSS 9.8**-A Heap Overflow vulnerability in WLAvalancheService component of Ivanti Avalanche before 6.4.3 allows a remote unauthenticated attacker to execute arbitrary commands.

2. **CVE-2024-24996 CVSS 9.8-**A Heap overflow vulnerability in WLInfoRailService component of Ivanti Avalanche before 6.4.3 allows an unauthenticated remote attacker to execute arbitrary commands.

Fixed Version:

- **Avalanche 6.4.3**

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to install the latest Avalanche version 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/Avalanche-6-4-3-Security-Hardening-and-CVEs-addressed?language=en_US