Smarttech
YOUR 24/7 SECURITY PARTNER

Dell Releases Security Updates for PowerScale InsightIQ - 12th May 2026

Document ID	SMA-Informative Cyber Alert
Document status	ISSUED
Authors	Alex Ciuta < alexandru.ciuta@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	12th May 2026
Issue Date	12th May 2026

Informative Cyber Alerts are reports created by Smarttech247 designed to inform customers about medium and low severity vulnerabilities, IOCs from certain attacks/breaches, and other information that could help companies be aware and protect against any attack.
The content of this report should be regarded as simply informative as it usually addresses products that have an auto-update option available for patches. It will be the customer's decision if it is necessary to follow any recommendation or disregard them as they are not currently applicable in the environment.

Overview

Dell PowerScale InsightIQ is affected by multiple high-impact security weaknesses across versions 5.0.0 through 6.2.0. These include an OS command injection flaw in versions 6.0.0–6.2.0, where improper neutralization of special elements could allow a high-privileged local attacker to execute arbitrary system commands, and an unnecessary privilege execution issue present from versions 5.0.0–6.2.0 that could enable the same class of attacker to escalate privileges. Together, these vulnerabilities increase the risk of command execution and privilege escalation on impacted systems, potentially compromising the integrity and security of the environment.

Technical Summary

DELL PowerScale InsightIQ

Proprietary Code CVEs	Description	CVSS Base Score
CVE-2026-35071	Dell PowerScale InsightIQ, versions 6.0.0 through 6.2.0, contains an improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Command execution.	8.2
CVE-2026-40638	Dell PowerScale InsightIQ, versions 5.0.0 through 6.2.0, contains an execution with unnecessary privileges vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to elevation of privileges.	6.7

Affected Products & Remediation

DELL PowerScale InsightIQ

CVEs Addressed	Product	Affected Versions	Remediated Versions
CVE-2026-35071	PowerScale InsightIQ	Versions 6.0.0 through 6.2.0	Version 6.3.0 or later
CVE-2026-40638	PowerScale InsightIQ	Versions 6.0.0 through 6.2.0	Version 6.3.0 or later

Recommendations

Smarttech247 team recommends the following actions to be taken:

- Upgrade to the latest versions in order to obtain a fix for these vulnerabilities.

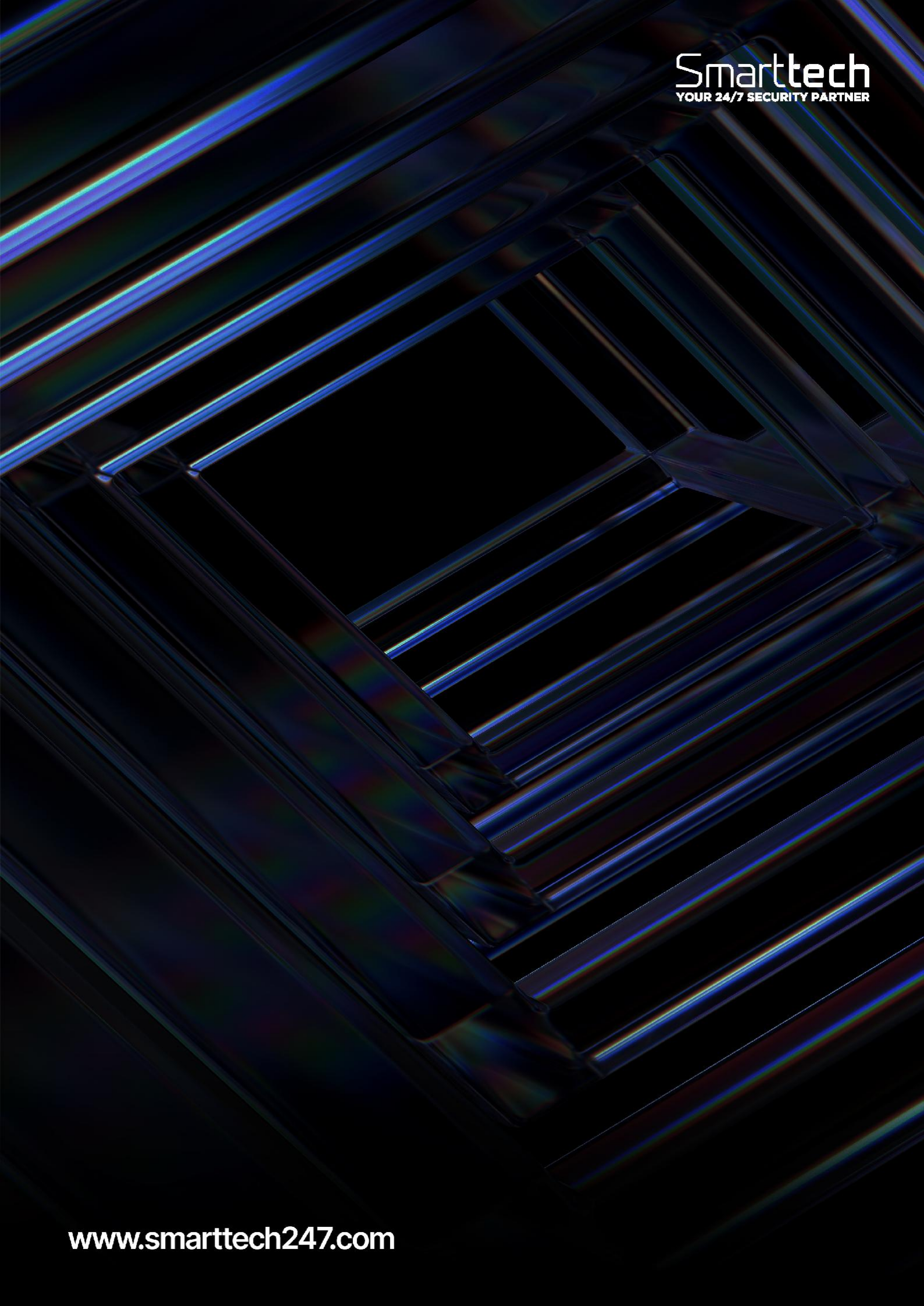
- Upgrade software and operating systems, applications, and firmware on network assets in a timely manner for prevention.
- Apply the Principle of Least Privilege to all systems and services.

References

1. https://www.dell.com/support/kbdoc/en-us/000463695/dsa-2026-208-security-update-for-dell-powerscale-insightiq-multiple-vulnerabilities
2. https://nvd.nist.gov/
3. https://www.cisa.gov/

CVEs:

CVE-2026-35071,
CVE-2026-40638


Smarttech
YOUR 24/7 SECURITY PARTNER
www.smarttech247.com