Smarttech
YOUR 24/7 SECURITY PARTNER

Dell Releases Security Updates for Networking OS10 - 22nd January 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	22nd January 2026
Issue Date	22nd January 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

Multiple security vulnerabilities have been identified in Dell Networking OS10. Successful exploitation of these vulnerabilities by malicious users could allow compromise of affected systems, potentially leading to unauthorized access, command execution, privilege escalation, information disclosure, or denial of service (DoS). Remediation is available through updated OS10 software releases to address these issues.

Technical Summary

Dell PowerStore T

Third-party Component	CVEs
linux	CVE-2024-47704, CVE-2024-57924, CVE-2024-58240, CVE-2025-23143, CVE-2025-23160, CVE-2025-37931, CVE-2025-37968, CVE-2025-38322, CVE-2025-38347, CVE-2025-38491, CVE-2025-38502, CVE-2025-38552, CVE-2025-38614, CVE-2025-38670, CVE-2025-38676, CVE-2025-38677, CVE-2025-38679, CVE-2025-38680, CVE-2025-38681, CVE-2025-38683, CVE-2025-38684, CVE-2025-38685, CVE-2025-38687, CVE-2025-38691, CVE-2025-38693, CVE-2025-38694, CVE-2025-38695, CVE-2025-38696, CVE-2025-38697, CVE-2025-38698, CVE-2025-38699, CVE-2025-38700, CVE-2025-38701, CVE-2025-38702, CVE-2025-38706, CVE-2025-38707, CVE-2025-38708, CVE-2025-38711, CVE-2025-38712, CVE-2025-38713, CVE-2025-38714, CVE-2025-38715, CVE-2025-38721, CVE-2025-38723, CVE-2025-38724, CVE-2025-38725, CVE-2025-38727, CVE-2025-38728, CVE-2025-38729, CVE-2025-38732, CVE-2025-38735, CVE-2025-38736, CVE-2025-39673, CVE-2025-39675, CVE-2025-39676, CVE-2025-39681, CVE-2025-39682, CVE-2025-39683, CVE-2025-39684, CVE-2025-39685, CVE-2025-39686, CVE-2025-39687, CVE-2025-39689, CVE-2025-39691, CVE-2025-39693, CVE-2025-39694, CVE-2025-39697, CVE-2025-39701, CVE-2025-39702, CVE-2025-39703, CVE-2025-39706, CVE-2025-39709, CVE-2025-39710, CVE-2025-39713, CVE-2025-39714, CVE-2025-39715, CVE-2025-39716, CVE-2025-39718, CVE-2025-39719, CVE-2025-39724, CVE-2025-39736, CVE-2025-39737, CVE-2025-39738, CVE-2025-39742, CVE-2025-39743, CVE-2025-39749, CVE-2025-39751, CVE-2025-39752, CVE-2025-39756, CVE-2025-39757, CVE-2025-39759, CVE-2025-39760, CVE-2025-39766, CVE-2025-39770, CVE-2025-39772, CVE-2025-39773, CVE-2025-39776, CVE-2025-39782, CVE-2025-39783, CVE-2025-39787, CVE-2025-39788, CVE-2025-39790, CVE-2025-39794, CVE-2025-39795, CVE-2025-39798, CVE-2025-39800, CVE-2025-39801, CVE-2025-39806, CVE-2025-39808, CVE-2025-39812, CVE-2025-39813, CVE-2025-39817, CVE-2025-39819, CVE-2025-39823, CVE-2025-39824, CVE-2025-39825, CVE-2025-39826, CVE-2025-39827, CVE-2025-39828, CVE-2025-39835, CVE-2025-39838, CVE-2025-39839, CVE-2025-39841, CVE-2025-39842, CVE-2025-39843, CVE-2025-39844, CVE-2025-39845, CVE-2025-39846, CVE-2025-39847, CVE-2025-39848, CVE-2025-39849, CVE-2025-39853, CVE-2025-39857, CVE-2025-39860, CVE-2025-39864, CVE-2025-39865, CVE-2025-39866, CVE-2025-40300, CVE-2024-26618, CVE-2024-26783, CVE-2024-26807, CVE-2024-28956, CVE-2024-35790, CVE-2024-36903,

	CVE-2024-36927, CVE-2024-43840, CVE-2024-46751, CVE-2024-53203, CVE-2024-53209, CVE-2024-57945, CVE-2025-21645, CVE-2025-21839, CVE-2025-21931, CVE-2025-22062, CVE-2025-37819, CVE-2025-37890, CVE-2025-37897, CVE-2025-37901, CVE-2025-37902, CVE-2025-37903, CVE-2025-37905, CVE-2025-37909, CVE-2025-37911, CVE-2025-37912, CVE-2025-37913, CVE-2025-37914, CVE-2025-37915, CVE-2025-37917, CVE-2025-37921, CVE-2025-37923, CVE-2025-37924, CVE-2025-37927, CVE-2025-37928, CVE-2025-37929, CVE-2025-37930, CVE-2025-37932, CVE-2025-37936, CVE-2025-37947, CVE-2025-37948, CVE-2025-37949, CVE-2025-37951, CVE-2025-37953, CVE-2025-37959, CVE-2025-37961, CVE-2025-37962, CVE-2025-37963, CVE-2025-37964, CVE-2025-37967, CVE-2025-37969, CVE-2025-37970, CVE-2025-37972, CVE-2025-37990, CVE-2025-37991
openssl	CVE-2025-9230, CVE-2025-9231, CVE-2025-9232
redis	CVE-2025-49844, CVE-2025-46817, CVE-2025-46818, CVE-2025-46819
tiff	CVE-2025-9900
openssh(pkix-ssh)	CVE-2025-61984
bind9	CVE-2025-8677, CVE-2025-40778, CVE-2025-40780
systemd	CVE-2025-4598

Proprietary Code CVEs	**Description**	**CVSS Base Score**
CVE-2025-46427	Dell SmartFabric OS10 Software, versions prior to 10.6.0.7, contain an Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Command execution.	8.8
CVE-2025-46428	Dell SmartFabric OS10 Software, versions prior to 10.6.0.7, contain an Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Code execution.	8.8

Affected Products & Remediation

Dell Networking OS10

Product	**Affected Versions**	**Remediated Versions**
Dell Networking OS10	Versions prior to 10.6.0.7	Version 10.6.0.7

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/000417961/dsa-2026-034-security-update-for-dell-networking-os10-vulnerabilities
2. https://nvd.nist.gov/
3. https://www.cisa.gov/

CVEs:

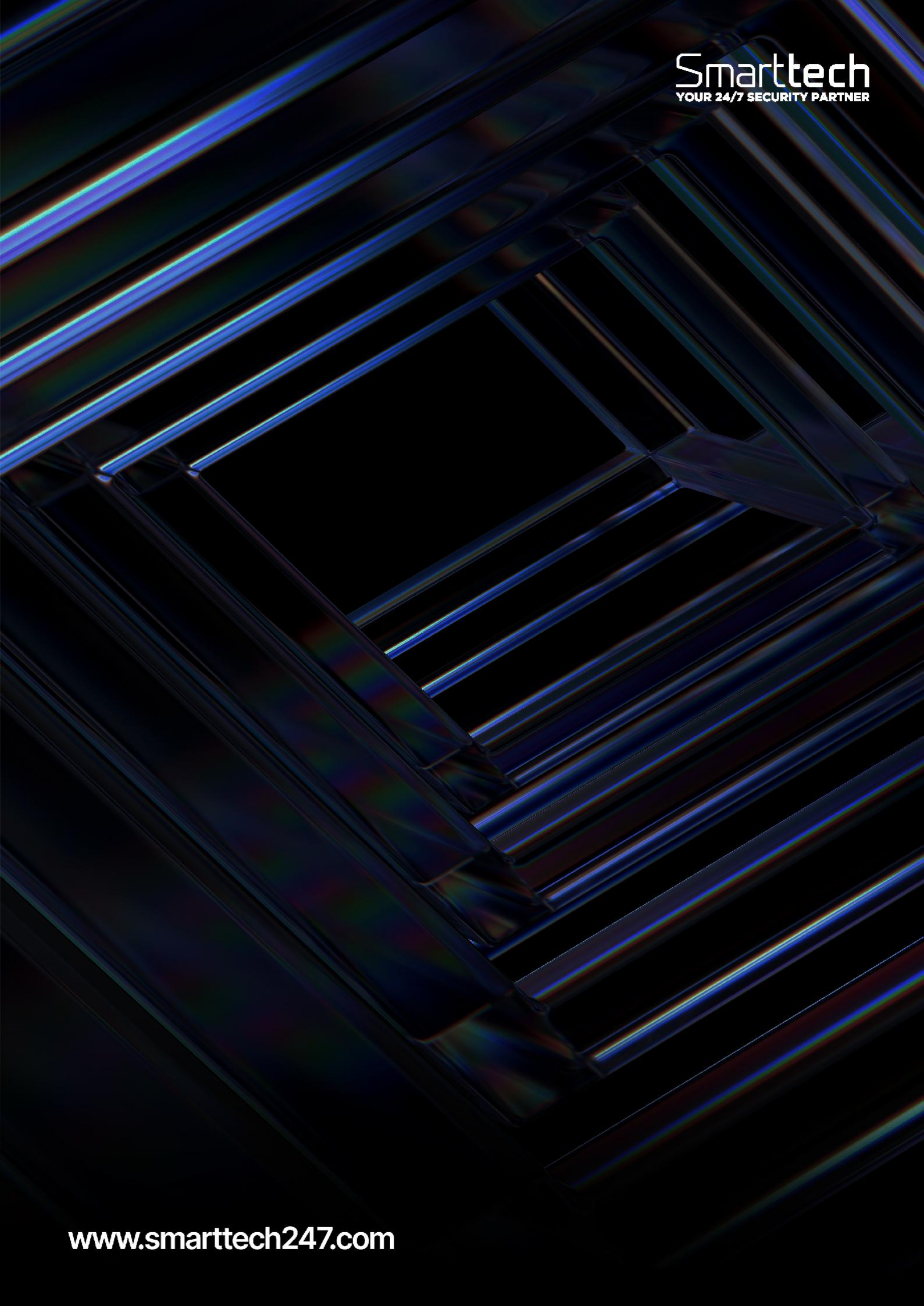
CVE-2024-47704,
CVE-2024-57924,
CVE-2024-58240,
CVE-2025-23143,
CVE-2025-23160,
CVE-2025-37931,
CVE-2025-37968,
CVE-2025-38322,
CVE-2025-38347,
CVE-2025-38491,
CVE-2025-38502,
CVE-2025-38552,
CVE-2025-38614,
CVE-2025-38670,
CVE-2025-38676,
CVE-2025-38677,
CVE-2025-38679,
CVE-2025-38680,
CVE-2025-38681,
CVE-2025-38683,
CVE-2025-38684,
CVE-2025-38685,
CVE-2025-38687,
CVE-2025-38691,
CVE-2025-38693,
CVE-2025-38694,
CVE-2025-38695,
CVE-2025-38696,
CVE-2025-38697,
CVE-2025-38698,
CVE-2025-38699,
CVE-2025-38700,
CVE-2025-38701,
CVE-2025-38702,
CVE-2025-38706,
CVE-2025-38707,
CVE-2025-38708,
CVE-2025-38711,

CVE-2025-38712,
CVE-2025-38713,
CVE-2025-38714,
CVE-2025-38715,
CVE-2025-38721,
CVE-2025-38723,
CVE-2025-38724,
CVE-2025-38725,
CVE-2025-38727,
CVE-2025-38728,
CVE-2025-38729,
CVE-2025-38732,
CVE-2025-38735,
CVE-2025-38736,
CVE-2025-39673,
CVE-2025-39675,
CVE-2025-39676,
CVE-2025-39681,
CVE-2025-39682,
CVE-2025-39683,
CVE-2025-39684,
CVE-2025-39685,
CVE-2025-39686,
CVE-2025-39687,
CVE-2025-39689,
CVE-2025-39691,
CVE-2025-39693,
CVE-2025-39694,
CVE-2025-39697,
CVE-2025-39701,
CVE-2025-39702,
CVE-2025-39703,
CVE-2025-39706,
CVE-2025-39709,
CVE-2025-39710,
CVE-2025-39713,
CVE-2025-39714,
CVE-2025-39715,
CVE-2025-39716,
CVE-2025-39718,
CVE-2025-39719,
CVE-2025-39724,
CVE-2025-39736,
CVE-2025-39737,
CVE-2025-39738,

CVE-2025-39742,
CVE-2025-39743,
CVE-2025-39749,
CVE-2025-39751,
CVE-2025-39752,
CVE-2025-39756,
CVE-2025-39757,
CVE-2025-39759,
CVE-2025-39760,
CVE-2025-39766,
CVE-2025-39770,
CVE-2025-39772,
CVE-2025-39773,
CVE-2025-39776,
CVE-2025-39782,
CVE-2025-39783,
CVE-2025-39787,
CVE-2025-39788,
CVE-2025-39790,
CVE-2025-39794,
CVE-2025-39795,
CVE-2025-39798,
CVE-2025-39800,
CVE-2025-39801,
CVE-2025-39806,
CVE-2025-39808,
CVE-2025-39812,
CVE-2025-39813,
CVE-2025-39817,
CVE-2025-39819,
CVE-2025-39823,
CVE-2025-39824,
CVE-2025-39825,
CVE-2025-39826,
CVE-2025-39827,
CVE-2025-39828,
CVE-2025-39835,
CVE-2025-39838,
CVE-2025-39839,
CVE-2025-39841,
CVE-2025-39842,
CVE-2025-39843,
CVE-2025-39844,
CVE-2025-39845,
CVE-2025-39846,

CVE-2025-39847,
CVE-2025-39848,
CVE-2025-39849,
CVE-2025-39853,
CVE-2025-39857,
CVE-2025-39860,
CVE-2025-39864,
CVE-2025-39865,
CVE-2025-39866,
CVE-2025-40300,
CVE-2024-26618,
CVE-2024-26783,
CVE-2024-26807,
CVE-2024-28956,
CVE-2024-35790,
CVE-2024-36903,
CVE-2024-36927,
CVE-2024-43840,
CVE-2024-46751,
CVE-2024-53203,
CVE-2024-53209,
CVE-2024-57945,
CVE-2025-21645,
CVE-2025-21839,
CVE-2025-21931,
CVE-2025-22062,
CVE-2025-37819,
CVE-2025-37890,
CVE-2025-37897,
CVE-2025-37901,
CVE-2025-37902,
CVE-2025-37903,
CVE-2025-37905,
CVE-2025-37909,
CVE-2025-37911,
CVE-2025-37912,
CVE-2025-37913,
CVE-2025-37914,
CVE-2025-37915,
CVE-2025-37917,
CVE-2025-37921,
CVE-2025-37923,
CVE-2025-37924,
CVE-2025-37927,
CVE-2025-37928,

CVE-2025-37929,
CVE-2025-37930,
CVE-2025-37932,
CVE-2025-37936,
CVE-2025-37947,
CVE-2025-37948,
CVE-2025-37949,
CVE-2025-37951,
CVE-2025-37953,
CVE-2025-37959,
CVE-2025-37961,
CVE-2025-37962,
CVE-2025-37963,
CVE-2025-37964,
CVE-2025-37967,
CVE-2025-37969,
CVE-2025-37970,
CVE-2025-37972,
CVE-2025-37990,
CVE-2025-37991,
CVE-2025-9230,
CVE-2025-9231,
CVE-2025-9232,
CVE-2025-49844,
CVE-2025-46817,
CVE-2025-46818,
CVE-2025-46819
CVE-2025-9900,
CVE-2025-61984,
CVE-2025-8677,
CVE-2025-40778,
CVE-2025-40780,
CVE-2025-4598,
CVE-2025-46427,
CVE-2025-46428


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