

2026.3 HF1 Release Notes

Build Number: 2026.3.1.7 [N-central]

Last updated: 02-August-2026



Important N-central 2026.3.1 HF1 (hotfix) includes important mitigation for CVE-2026-18556. For more information, please see our [release notes](#).



Important The Windows Agent installer is now 180 MB, up from 90 MB, due to new additions in this release. Plan for higher bandwidth use and stagger your agent upgrades to reduce network load.

For full release information:

To review all new features, enhancements, and fixes included in the 2026.3 release, see the [2026.3 Release Notes](#).

Bug Fixes

A range of high-impact bugs have been resolved in this release. Be sure to review the full list included below for more details.

Search bug fixes...

Category	Updated Summary	Issue Key
Core	Veeam 13 Automatic Service Discovery Summary: N-central now detects and automatically onboards Veeam Backup & Replication 13 installations. Issue: Previously, devices running Veeam 13 were not recognized by the service template discovery process, preventing Veeam monitoring services from being deployed automatically. Partners had to manually	NCCF-2124781

Category	Updated Summary	Issue Key
	configure monitoring after installing Veeam 13. Fix: The N-central Agent has been updated to recognize Veeam 13 and automatically deploy the appropriate Veeam monitoring service templates, restoring the expected onboarding experience.	
Automation Manager	Updated Built-in Veeam Monitoring Services for Veeam 13 Summary: Updated the following built-in Veeam monitoring services to support Veeam Backup & Replication 13: ■ Veeam Failed Jobs ■ Veeam Job Monitor ■ Veeam Sure Job Monitor Issue: Veeam 13 requires PowerShell 7 (pwsh) for its PowerShell modules. The existing monitoring services used Windows PowerShell, preventing them from collecting monitoring data correctly in Veeam 13 environments. Fix: The Automation Manager policies have been updated to execute using PowerShell 7, ensuring the built-in monitoring services function correctly with Veeam 13 while remaining compatible with earlier supported Veeam versions.	AM-6417
Automation Manager	AMP Monitoring: Resolved Invalid Script Format Errors Summary: Resolved an issue that could cause custom Automation Manager Policy (AMP) monitoring services to report a 201: Invalid Script Format error, even when the underlying scripts were valid. Issue: In certain environments, an invalid Automation Manager token registry state could cause AMP to incorrectly interpret valid monitoring scripts as invalid, resulting in monitoring failures across affected devices.	AM-6515

Category	Updated Summary	Issue Key
	Fix: This update corrects the Automation Manager token registry handling to prevent invalid registry states from impacting script execution. AMP monitoring services now process valid scripts correctly, eliminating these erroneous validation failures.	
Patch Management	Patch Management: Immediate Pre-download Maintenance Windows No Longer Become Stuck Summary: Resolved an issue where immediate pre-download maintenance windows could become permanently stuck in the queue when there were no approved patches available to download. Issue: Previously, if a pre-download maintenance window found no approved patches, the schedule could fail to complete correctly, preventing subsequent maintenance windows from running until manual intervention. Fix: This update ensures immediate pre-download maintenance windows complete successfully even when there is nothing to download, allowing queued maintenance windows to continue processing as expected. Patch-on-Boot maintenance windows are unaffected by this change.	PMCM-11816
Security	MFA reset and disable options unavailable for MSP SSO users Summary: Resolved an issue where administrators managing users configured with MSP SSO were unable to reset or disable multi-factor authentication (MFA) from the user interface. Issue: In N-central, the "Reset MFA" and "Disable Two-Factor Authentication" options were missing for users configured with MSP SSO, preventing administrators from managing MFA through the UI. Fix: Restored both the "Reset MFA" and "Disable Two-Factor Authentication" options for MSP SSO users.	NCCF-2544553

