CyberDudeBivash — DSM Emergency Change Ticket

CVE-2025-43995 | Dell Storage Manager (DSM) API Authentication Bypass

Pre-Change Checklist

Task	Status / Notes
■ Verify current DSM version (< 20.1.21 is vulnerable)	
■ Backup configuration & array metadata	
■ Validate backup integrity (checksum + test restore)	
■ Notify impacted teams (storage, network, SOC)	
■ Schedule 30-min maintenance window	

Change Implementation Plan

1. Stop DSM services on management host.
2. Install patched version 2020 R1.22 or later.
3. Restart DSM collector and web services.
4. Validate version upgrade in DSM UI.
5. Rotate DSM admin passwords and stored array credentials.
6. Verify that /ApiProxy endpoints are blocked externally.
7. Validate DSM access and array communication.
8. Capture logs and screenshot for change evidence.

Rollback Plan

If upgrade fails or DSM unresponsive:
1. Restore previous version from verified backup.
2. Re-import config and revalidate storage connectivity.
3. Notify SOC and management immediately.
4. Apply WAF rule blocking /ApiProxy paths until issue is resolved.

Post-Change Verification

- Confirm DSM version displays 2020 R1.22+.
- Confirm no open /ApiProxy endpoints.
- Review logs for unauthorized access attempts.
- Validate array communication and automation jobs.
- Mark change ticket as 'Completed & Verified'.

Approvals

Role	Name	Signature	Timestamp
Change Requestor			

Change Approver			
Implementation Engineer			
SOC Reviewer			