INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-01 18:43 UTC

Brute-Force Campaign Targets Dashlane Accounts, Triggering Lockouts and Exposing Password Manager Vault Risk

THREAT CAMPAIGN | **HIGH** | CVSS 5.0

SCC Item ID	SCC-CAM-2026-0389
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	5.0
Affected Products	Dashlane Password Manager (all account types, enterprise and consumer)
Published	2026-06-01T14:17:13
Discovery Source	Rss

Executive Summary

On May 31, 2026, attackers launched a brute-force campaign against Dashlane user accounts, triggering automated lockouts across both enterprise and consumer accounts. The core business risk extends beyond the lockouts themselves: a successfully compromised Dashlane master account exposes every credential stored in that vault, potentially granting attackers access to all enterprise systems whose passwords are managed there. Limited public disclosure from Dashlane means security teams cannot yet determine full campaign scope or confirm whether any vaults were accessed.

Technical Analysis

Attackers used credential stuffing and distributed brute-force techniques (MITRE T1110, T1110.001, T1110.003, T1110.004) against Dashlane authentication endpoints, originating from foreign IP addresses and unrecognized devices. Dashlane's automated suspension controls triggered as designed, resulting in account lockouts. No CVE has been assigned. Relevant weaknesses include CWE-307 (improper restriction of excessive authentication attempts), CWE-521 (weak password requirements for master passwords), and CWE-308 (use of single-factor authentication). Successful master password compromise would enable offline vault decryption and bulk credential harvesting (T1555, T1555.005). Threat actors may leverage previously breached credentials (T1586.002) or valid accounts (T1078) for follow-on access. Patch status: no vendor patch applicable; mitigations are configuration and policy controls. No CVSS vendor score or EPSS data is available for this campaign.

Action Checklist

1. Step 1: Containment, Identify all enterprise Dashlane accounts and verify which accounts triggered lockouts. Require immediate master password resets for any account that received a lockout notification or was accessed from an unrecognized device. Enforce NIST SP 800-53 AC-7 (Unsuccessful Logon Attempts) by confirming Dashlane's lockout thresholds align with your organization's policy.
2. Step 2: Detection, Query IdP and SSO logs for authentication failures against accounts known to use Dashlane as a credential store. Review Dashlane admin console (if Business/Teams tier) for suspended account alerts, unrecognized device logins, and foreign IP access events. Look for MITRE T1110 indicators: high-frequency failed logins from single or rotating IPs. Cross-reference AU-2 (Event Logging) and CIS 8.2 (Collect Audit Logs) to confirm Dashlane activity is captured in your SIEM. Apply D3-LAM (Local Account Monitoring) to surface anomalous Dashlane-associated account activity.
3. Step 3: Eradication, Enforce strong, unique master passwords meeting or exceeding NIST SP 800-63B length requirements (minimum 15 characters recommended) across all enterprise Dashlane accounts, addressing CWE-521. Enable and enforce multi-factor authentication on all Dashlane accounts per CIS 6.3 (Require MFA for Externally-Exposed Applications) and CIS 6.5 (Require MFA for Administrative Access). Apply D3-MFA and D3-CH (Credential Hardening) countermeasures. Rotate high-value credentials stored in vaults for accounts confirmed as targeted, per D3-CRO (Credential Rotation).
4. Step 4: Recovery, Validate that locked-out accounts have completed master password resets before reinstatement. Confirm MFA is active on restored accounts before re-enabling vault access. Monitor Dashlane admin console and SIEM for recurrence over the following 14 days. Verify that AU-6 (Audit Record Review, Analysis, and Reporting) cadence covers Dashlane-related authentication events post-incident.
5. Step 5: Post-Incident, Conduct a tabletop review of centralized password manager risk: a single compromised vault is a single point of failure for all stored credentials (NIST SP 800-53 AC-5, Separation of Duties, and AC-6, Least Privilege, both apply to vault access scoping). Evaluate whether privileged and shared credentials should be separated from personal vaults. Document findings against CIS 7.1 (Establish and Maintain a Vulnerability Management Process) and update your authentication hardening policy to address CWE-307 and CWE-308 gaps organization-wide.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to CISO and legal counsel immediately if Dashlane admin console 'vault_item_accessed' events confirm any successful authentication preceded lockout for accounts storing credentials to regulated systems (PII, PHI, PCI-scoped, or financial data), as this constitutes a probable breach triggering regulatory notification assessment under applicable state breach laws, HIPAA, or PCI DSS v4.0 Requirement 12.10.

Recovery Notes	Before restoring any locked-out account, verify three conditions in sequence via Dashlane admin console: master password was reset after May 31, 2026; MFA is confirmed active on the account; and no unrecognized devices remain registered. Monitor the Dashlane admin console audit log and IdP sign-in logs daily for 14 days post-recovery, specifically watching for renewed high-frequency login failures from the same IP ranges identified during the May 31 campaign. If Dashlane publishes a formal incident report or identifies specific attacker infrastructure, retroactively search retained logs from the attack window against those indicators to determine whether any pre-lockout vault access occurred that was not yet detected.
Forensic Artifacts	Dashlane Business admin console audit log export (JSON/CSV) covering May 31, 2026 ±48 hours — primary source for 'login_failed', 'account_suspended', 'device_added', and 'vault_item_accessed' events with originating IP addresses, timestamps, and device fingerprints; this log is the only source that can confirm whether a successful vault authentication preceded lockout. | IdP/SSO authentication logs (Okta System Log or Azure AD Sign-In logs) for all Dashlane-enrolled accounts during the attack window — cross-referencing failed Dashlane logins against downstream SSO activity reveals whether attackers pivoted from Dashlane credentials to enterprise SSO sessions before lockout triggered. | Dashlane admin console device registry snapshot for each targeted account (pre-reset) — attacker-registered devices will appear as unrecognized entries with non-organizational OS/browser fingerprints and originating IPs inconsistent with the user's normal geolocations; this is the primary artifact for confirming attacker device persistence. | Dashlane shared collection membership export (Admin Console → Sharing Center) for all targeted accounts — determines the true blast radius beyond individual vault contents by mapping which shared credentials (service accounts, shared infrastructure passwords) were accessible to each compromised account. | Firewall or proxy egress logs for outbound HTTPS connections from endpoints running Dashlane browser extensions or desktop clients to *.dashlane.com API endpoints during the attack window — vault sync traffic from attacker-controlled devices would appear as unexpected source IPs initiating sync sessions, distinct from the legitimate user's normal device traffic.

Per-Action IR Details

Step 1: Containment — Identify all enterprise Dashlane accounts and verify which accounts triggered lockouts. Require immediate master password resets for any account that received a lockout notification or was accessed from an unrecognized device. Enforce NIST AC-7 (Unsuccessful Logon Attempts) by confirming Dashlane's lockout thresholds align with your organization's policy.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-7 (Unsuccessful Logon Attempts), NIST IR-4 (Incident Handling), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: Export the Dashlane Business admin console member list to CSV (Admin Console → Members → Export). Cross-reference against your HR/identity source of truth using a PowerShell one-liner: `Compare-Object (Import-Csv dashlane_members.csv -Header email) (Get-ADUser -Filter * -Properties mail | Select mail)` to surface unmanaged or shadow accounts. For lockout verification without SIEM, query Dashlane admin console under Security → Account Activity filtered by 'Account suspended' and 'Unrecognized device' events and screenshot with timestamps before any resets occur.

Evidence: Before forcing master password resets, capture: (1) Dashlane Business admin console export of all 'Account suspended' and 'Unusual login attempt' alerts with originating IP addresses and timestamps from the May 31, 2026 window; (2) the full list of devices registered to each locked-out account (Admin Console → Member detail → Devices) to establish pre-reset device baseline; (3) IdP/SSO authentication logs for the same accounts during the

attack window, preserving raw log files before any retention rollover. Resetting master passwords before capturing device lists destroys the ability to identify attacker-registered devices.

Step 2: Detection — Query IdP and SSO logs for authentication failures against accounts known to use Dashlane as a credential store. Review Dashlane admin console (if Business/Teams tier) for suspended account alerts, unrecognized device logins, and foreign IP access events. Look for MITRE T1110 indicators: high-frequency failed logins from single or rotating IPs. Cross-reference AU-2 (Event Logging) and CIS 8.2 (Collect Audit Logs) to confirm Dashlane activity is captured in your SIEM. Apply D3-LAM (Local Account Monitoring) to surface anomalous Dashlane-associated account activity.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, use the Dashlane Business admin console audit log export (JSON/CSV) and run: `jq '[.[] | select(.event_type == "login_failed" or .event_type == "account_suspended" or .event_type == "device_added")] | group_by(.ip_address) | map({ip: .[0].ip_address, count: length}) | sort_by(-.count)' dashlane_audit.json` to surface IPs generating the highest failure volume. For IdP correlation, export Okta System Log or Azure AD Sign-In logs as CSV and filter on ResultType != 0 (Azure) or `eventType eq "user.session.start"` with outcome FAILURE (Okta) joined on the Dashlane account email list. Deploy the public Sigma rule for T1110 (Brute Force: Password Spraying) against exported logs using sigma-cli with the generic log backend.

Evidence: Capture before analysis: (1) Dashlane Business admin console audit log export covering May 31, 2026 ±48 hours — specifically events of type 'login_failed', 'account_suspended', 'device_added', and 'vault_item_accessed'; (2) raw IdP sign-in logs (Okta System Log JSON or Azure AD Sign-In logs) for all accounts in the Dashlane member export, covering the same window; (3) DNS query logs or firewall egress logs for outbound connections from endpoints running the Dashlane browser extension or desktop app to Dashlane API endpoints (*.dashlane.com) during the attack window, which may reveal whether any vault sync occurred post-lockout; (4) list of IP addresses from failed Dashlane login attempts for threat intel enrichment against known credential-stuffing infrastructure.

Step 3: Eradication — Enforce strong, unique master passwords meeting or exceeding NIST SP 800-63B length requirements (minimum 15 characters recommended) across all enterprise Dashlane accounts, addressing CWE-521. Enable and enforce multi-factor authentication on all Dashlane accounts per CIS 6.3 (Require MFA for Externally-Exposed Applications) and CIS 6.5 (Require MFA for Administrative Access). Apply D3-MFA and D3-CH (Credential Hardening) countermeasures. Rotate high-value credentials stored in vaults for accounts confirmed as targeted, per D3-CRO (Credential Rotation).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IA-5 (Authenticator Management), NIST IA-2 (Identification and Authentication), NIST AC-2 (Account Management), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 5.2 (Use Unique Passwords)

Compensating: Enforce MFA via Dashlane Business admin console (Settings → Security → Two-Factor Authentication → Required for all members) — this is a built-in control requiring no additional tooling. For credential rotation of high-value secrets stored in targeted vaults, generate a prioritized rotation list by exporting vault item categories from the admin console and sorting by item type (privileged credentials, shared secrets, API keys) before beginning resets. Without PAM tooling, use a structured spreadsheet tracking: account name, credential type, rotation status, and confirming employee — assign ownership to each line item and require completion within 24 hours for any vault confirmed as accessed by an unrecognized device.

Evidence: Before rotating credentials, capture: (1) Dashlane admin console report of 'vault_item_accessed' events for targeted accounts during the May 31 window — this determines whether a successful login preceded lockout and which specific vault items were potentially exposed; (2) a snapshot of all shared collection memberships for targeted accounts (Admin Console → Sharing Center) to scope which credentials were accessible, not just which the user

personally stored; (3) for any account where an unrecognized device was added before lockout triggered, capture the device fingerprint details (OS, browser, Dashlane client version) as these may match attacker infrastructure seen in other campaigns.

Step 4: Recovery — Validate that locked-out accounts have completed master password resets before reinstatement. Confirm MFA is active on restored accounts before re-enabling vault access. Monitor Dashlane admin console and SIEM for recurrence over the following 14 days. Verify that AU-6 (Audit Record Review, Analysis, and Reporting) cadence covers Dashlane-related authentication events post-incident.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST IR-4 (Incident Handling), NIST CA-7 (Continuous Monitoring), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: Build a 14-day monitoring checklist as a recurring daily task: pull Dashlane admin console audit log each morning and run the same jq IP-frequency query from Step 2 to detect renewed brute-force activity. Set a Dashlane Business admin console email alert (Settings → Notifications) for 'Account suspended' and 'Unrecognized device' events to ensure real-time notification without SIEM integration. Create a simple reinstatement gate: no account is re-enabled until the responder verifies via admin console that (a) master password was reset after May 31, 2026, (b) MFA method is confirmed active, and (c) no unrecognized devices remain registered — document each account's gate passage with a timestamp.

Evidence: Before reinstating any account, capture a post-reset baseline: (1) Dashlane admin console device list for each restored account confirming only known, authorized devices remain registered; (2) MFA enrollment confirmation screenshot from admin console (member detail → Two-Factor Authentication: Enabled); (3) first successful post-reset login timestamp and originating IP from IdP/SSO logs to establish a clean-state baseline for the 14-day monitoring window. Retain all pre-reset evidence collected in Steps 1-3 in a dedicated incident folder — do not overwrite with post-recovery logs.

Step 5: Post-Incident — Conduct a tabletop review of centralized password manager risk: a single compromised Dashlane master account is a single point of failure for all stored credentials (NIST AC-5, Separation of Duties, and AC-6, Least Privilege, both apply to vault access scoping). Evaluate whether privileged and shared credentials should be separated from personal vaults. Document findings against CIS 7.1 (Establish and Maintain a Vulnerability Management Process) and update your authentication hardening policy to address CWE-307 and CWE-308 gaps organization-wide.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST AC-5 (Separation of Duties), NIST AC-6 (Least Privilege), NIST IR-4 (Incident Handling), NIST RA-3 (Risk Assessment), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Structure the tabletop as a 90-minute working session with three outputs: (1) a Dashlane shared collection audit — export current sharing memberships and identify any privileged credentials (domain admin, cloud root, financial systems) co-mingled in personal or broadly-shared collections; (2) a written decision on whether to migrate privileged credentials to a dedicated secrets manager (HashiCorp Vault free tier or Bitwarden Secrets Manager OSS) separate from the personal Dashlane vault, reducing the blast radius of a single compromised master account; (3) a one-page policy addendum mandating MFA on all password manager accounts and prohibiting master passwords below 15 characters, approved by the security lead. Document the tabletop with dated meeting notes and attach to the incident record.

Evidence: For the post-incident record, compile: (1) final count of accounts locked out on May 31, 2026 vs. total enterprise Dashlane seats — this quantifies campaign scope; (2) list of any vault items confirmed accessed during the attack window (from Step 3 vault_item_accessed evidence) to document actual vs. potential exposure; (3) before-and-after MFA enrollment rates from Dashlane admin console (pre-incident baseline if available vs. post-eradication enforcement confirmation); (4) a gap analysis comparing your organization's lockout threshold policy against Dashlane's enforced threshold to document the AC-7 alignment finding for audit purposes.

Detection Guidance

Query your SIEM or IdP logs for repeated failed authentication events against accounts known to use Dashlane as a credential store. Key indicators: multiple failed logins within short windows from foreign or unrecognized IPs (T1110 pattern), device registration alerts from Dashlane for unrecognized endpoints, and automated account suspension notifications. In the Dashlane Business/Teams admin console, review the Security Dashboard for suspended accounts and login anomalies. If Dashlane authentication events are forwarded to your SIEM, look for event sequences matching T1110.003 (Password Spraying) or T1110.004 (Credential Stuffing): low-and-slow failures across many accounts, or high-volume failures against a single account. Apply D3-LAM (Local Account Monitoring) and D3-SFA (System File Analysis) to detect post-compromise credential access if vault data is suspected accessed. No confirmed IOCs (IP addresses, hashes, domains) have been publicly released for this campaign as of the reporting date; monitor BleepingComputer and Dashlane's official security communications for updates. Source quality is T3/secondary, human validation of current reporting accuracy is recommended before treating specific IOCs as confirmed.

Indicators of Compromise

Type	Value	Context	Confidence
IP	`Not publicly released`	Foreign IP addresses reported as attack sources in BleepingComputer reporting — no specific IPs confirmed or published as of reporting date	LOW

Framework Mappings

MITRE-ATTACK

- **T1110** — Brute Force
- **T1555.005** — Password Managers
- **T1555** — Credentials from Password Stores
- **T1586.002** — Email Accounts
- **T1110.004** — Credential Stuffing
- **T1110.003** — Password Spraying
- **T1078** — Valid Accounts
- **T1110.001** — Password Guessing

NIST-800-53R5

- **AC-7** — Unsuccessful Logon Attempts
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-2** — Account Management
- **AC-6** — Least Privilege

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1110	Brute Force	Credential-Access
T1555.005	Password Managers	Credential-Access
T1555	Credentials from Password Stores	Credential-Access
T1586.002	Email Accounts	Resource-Development
T1110.004	Credential Stuffing	Credential-Access
T1110.003	Password Spraying	Credential-Access
T1078	Valid Accounts	Defense-Evasion
T1110.001	Password Guessing	Credential-Access

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/dashlane-password-ma...	T3
Dashlane: Password management & credential security platform	https://www.dashlane.com/	T3
Security analysis of Password Managers (Bitwarden, LastPass ...	https://www.reddit.com/r/selfhosted/comments/1r7x5w2/security_analy...	T3
Breaches & Alerts - Dashlane	https://www.dashlane.com/blog/category/tech-news/breaches-and-alerts	T3

Source	URL	Tier
Security at Dashlane	https://support.dashlane.com/hc/en-us/articles/360012686840-Securit...	T3

Generated 2026-06-01 18:43 UTC by TJS Security Command Center