# DSA-2026-060: Security Update for Dell PowerProtect Data Domain Multiple Vulnerabilities

Summary: Dell PowerProtect Data Domain remediation is available for multiple security vulnerabilities that could be exploited by malicious users to compromise the affected system.





## Impact

High

## Additional Details

The Affected Products and Remediation table above may not be a comprehensive list of all affected supported versions and may be updated as more information becomes available.

## Details

| Third-Party Component | CVEs | More Information |
|---|---|---|
| Apache Commons FileUpload | CVE-2025-48976 | https://nvd.nist.gov/vuln/search |
| inftrees.c in zlib | CVE-2016-9840 | https://nvd.nist.gov/vuln/search |
| GNU Coreutils | CVE-2025-5278 | https://nvd.nist.gov/vuln/search |
| libgcrypt's RSA | CVE-2024-2236 | https://nvd.nist.gov/vuln/search |
| PostgreSQL | CVE-2025-4207 | https://nvd.nist.gov/vuln/search |
| Python | CVE-2024-12718, CVE-2025-0938, CVE-2025-4516, CVE-2025-6069 | https://nvd.nist.gov/vuln/search |
| SQLite | CVE-2025-6965 | https://nvd.nist.gov/vuln/search |
| Libssh | CVE-2025-4877, CVE-2025-4878,CVE-2025-5372, CVE-2025-5318 | https://nvd.nist.gov/vuln/search |
| systemd-coredump | CVE-2025-4598 | https://nvd.nist.gov/vuln/search |

| Third-Party Component | CVEs | More Information |
|---|---|---|
| Linux kernel | CVE-2025-37925, CVE-2025-37805, CVE-2025-37803, CVE-2025-37802, CVE-2025-37801, CVE-2025-37800, CVE-2025-37785, CVE-2025-23136, CVE-2025-22063, CVE-2025-22038, CVE-2025-22037, CVE-2025-22027, CVE-2025-22018, CVE-2025-22007, CVE-2025-21996, CVE-2025-21993 | https://nvd.nist.gov/vuln/search |
| OpenSSL | CVE-2024-9143 | https://nvd.nist.gov/vuln/search |
| linux-pam | CVE-2025-6020 | https://nvd.nist.gov/vuln/search |
| Requests | CVE-2024-47081 | https://nvd.nist.gov/vuln/search |
| libxml2 | CVE-2025-49794, CVE-2025-49796, CVE-2025-7425, CVE-2025-6021, CVE-2025-6170 | https://nvd.nist.gov/vuln/search |

| Proprietary Code CVEs | Description | CVSS Base Score | CVSS Vector String |
|---|---|---|---|
| CVE-2026-26944 | Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.6, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60 contain a missing authentication for critical function vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges. Exploitation requires an authenticated user to perform a specific action. | 8.8 | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H |
| CVE-2026-23853 | Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.50, contain a use of weak credentials vulnerability. An unauthenticated attacker with local access could potentially exploit this vulnerability, leading to unauthorized access to the system. | 8.4 | CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |

| Proprietary Code CVEs | Description | CVSS Base Score | CVSS Vector String |
|---|---|---|---|
| CVE-2026-26354 | Dell PowerProtect Data Domain with Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.6, LTS2025 release version 8.3.1.0 through 8.3.1.10, LTS2024 release versions 7.13.1.0 through 7.13.1.60, contain a stack-based Buffer Overflow vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution. | 8.2 | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H |
| CVE-2025-36568 | Dell PowerProtect Data Domain BoostFS for client of Feature Release versions 7.7.1.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.50, contain an insufficiently protected credentials vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to credential exposure. The attacker may be able to use the exposed credentials to access the system with privileges of the compromised account. | 7.8 | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H |
| CVE-2026-23775 | Dell PowerProtect Data Domain appliances with Data Domain Operating System (DD OS) of Feature Release versions 8.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.10 contain an insertion of sensitive information into log file vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to credential exposures. Authentication attempts as the compromised user would need to be authorized by a high privileged DD user. This vulnerability only affects systems with retention lock enabled. | 7.6 | CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:H/A:H |
| CVE-2026-23774 | Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.10, LTS2024 release versions 7.13.1.0 through 7.13.1.40, contain an OS command injection vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution. | 7.2 | CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H |
| CVE-2026-24504 | Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.6, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60 contain an improper input validation vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges. | 7.2 | CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H |
| CVE-2026-24505 | Dell PowerProtect Data Domain, versions 8.5 through 8.6 contain an improper input validation vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges. | 7.2 | CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H |

| Proprietary Code CVEs | Description | CVSS Base Score | CVSS Vector String |
|---|---|---|---|
| CVE-2026-24506 | Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.6, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60 contain an OS command injection vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution as root. | 7.2 | CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H |
| CVE-2026-26943 | Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.6, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60 contain an OS command injection vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges. | 7.2 | CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H |
| CVE-2026-23778 | Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.50, contain a command injection vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability to gain root-level access. | 7.2 | CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H |
| CVE-2026-23776 | Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60, contain(s) an Improper Certificate Validation vulnerability in certificate-based login. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Elevation of privileges. | 7.2 | CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H |
| CVE-2026-26942 | Dell PowerProtect Data Domain, versions 8.5 through 8.6 contain(s) an Improper Neutralization of Special Elements used in an OS Command ('OS command injection vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges. | 6.7 | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H |
| CVE-2026-22761 | Dell PowerProtect Data Domain, versions 8.5 through 8.6 contain a command injection vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges. | 6.7 | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H |

| Proprietary Code CVEs | Description | CVSS Base Score | CVSS Vector String |
|---|---|---|---|
| CVE-2026-26951 | Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.6, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60 contain a stack-based buffer overflow vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges. | 6.7 | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H |
| CVE-2026-23779 | Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.50, contain a command injection vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability to gain root-level access. | 6.7 | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H |
| CVE-2026-35153 | Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7.0.0, LTS2025 release versions 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60 contain an improper neutralization of argument delimiters in a command ('argument injection') vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges. | 6.7 | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H |
| CVE-2026-35072 | Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7.0.0, LTS2025 release versions 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60 contain 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 arbitrary command execution with root privileges. | 6.7 | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H |
| CVE-2026-35074 | Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7.0.0, LTS2025 release versions 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60 contain an improper neutralization of special elements used in an OS Command Injection vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges. | 6.7 | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H |

| Proprietary Code CVEs | Description | CVSS Base Score | CVSS Vector String |
|---|---|---|---|
| CVE-2026-35073 | Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7.0.0, LTS2025 release versions 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60 contain an improper neutralization of special elements used in an OS command injection vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges. | 6.7 | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H |
| CVE-2025-46607 | Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 8.4 through 8.5 contain an improper authentication vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access. | 6.6 | CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H |
| CVE-2025-46641 | Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 8.4 through 8.5 contain an improper authentication vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access. | 6.6 | CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H |
| CVE-2026-35154 | Dell PowerProtect Data Domain appliances, versions 7.7.1.0 through 8.7.0.0, LTS2025 release versions 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60 contain an improper privilege management vulnerability in IDRAC. A high privileged attacker with local access could potentially exploit this vulnerability, leading to elevation of privileges to access unauthorized delete operation in IDRAC. | 6.3 | CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H |
| CVE-2025-46605 | Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 8.4 through 8.5 contain a session fixation vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access. | 6.2 | CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:L |
| CVE-2025-46606 | Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 8.4 through 8.5 contain an improper restriction of excessive authentication attempts vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access. | 6.2 | CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:L |

| Proprietary Code CVEs | Description | CVSS Base Score | CVSS Vector String |
|---|---|---|---|
| CVE-2026-28263 | Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.50, contain a cross-site Scripting vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Script injection. | 5.9 | CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:L |
| CVE-2026-23777 | Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.50, contain an exposure of sensitive information to an unauthorized actor vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to information exposure. | 4.3 | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N |

| Proprietary Code CVEs | Description | CVSS Base Score | CVSS Vector String |
|---|---|---|---|
| CVE-2026-26944 | Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.6, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60 contain a missing authentication for critical function vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges. Exploitation requires an authenticated user to perform a specific action. | 8.8 | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H |
| CVE-2026-23853 | Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.50, contain a use of weak credentials vulnerability. An unauthenticated attacker with local access could potentially exploit this vulnerability, leading to unauthorized access to the system. | 8.4 | CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| CVE-2026-26354 | Dell PowerProtect Data Domain with Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.6, LTS2025 release version 8.3.1.0 through 8.3.1.10, LTS2024 release versions 7.13.1.0 through 7.13.1.60, contain a stack-based Buffer Overflow vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution. | 8.2 | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H |

| Proprietary Code CVEs | Description | CVSS Base Score | CVSS Vector String |
|---|---|---|---|
| CVE-2025-36568 | Dell PowerProtect Data Domain BoostFS for client of Feature Release versions 7.7.1.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.50, contain an insufficiently protected credentials vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to credential exposure. The attacker may be able to use the exposed credentials to access the system with privileges of the compromised account. | 7.8 | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H |
| CVE-2026-23775 | Dell PowerProtect Data Domain appliances with Data Domain Operating System (DD OS) of Feature Release versions 8.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.10 contain an insertion of sensitive information into log file vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to credential exposures. Authentication attempts as the compromised user would need to be authorized by a high privileged DD user. This vulnerability only affects systems with retention lock enabled. | 7.6 | CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:H/A:H |
| CVE-2026-23774 | Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.10, LTS2024 release versions 7.13.1.0 through 7.13.1.40, contain an OS command injection vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution. | 7.2 | CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H |
| CVE-2026-24504 | Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.6, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60 contain an improper input validation vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges. | 7.2 | CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H |
| CVE-2026-24505 | Dell PowerProtect Data Domain, versions 8.5 through 8.6 contain an improper input validation vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges. | 7.2 | CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H |
| CVE-2026-24506 | Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.6, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60 contain an OS command injection vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution as root. | 7.2 | CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H |

| Proprietary Code CVEs | Description | CVSS Base Score | CVSS Vector String |
|---|---|---|---|
| CVE-2026-26943 | Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.6, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60 contain an OS command injection vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges. | 7.2 | CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H |
| CVE-2026-23778 | Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.50, contain a command injection vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability to gain root-level access. | 7.2 | CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H |
| CVE-2026-23776 | Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60, contain(s) an Improper Certificate Validation vulnerability in certificate-based login. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Elevation of privileges. | 7.2 | CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H |
| CVE-2026-26942 | Dell PowerProtect Data Domain, versions 8.5 through 8.6 contain(s) an Improper Neutralization of Special Elements used in an OS Command ('OS command injection vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges. | 6.7 | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H |
| CVE-2026-22761 | Dell PowerProtect Data Domain, versions 8.5 through 8.6 contain a command injection vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges. | 6.7 | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H |
| CVE-2026-26951 | Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.6, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60 contain a stack-based buffer overflow vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges. | 6.7 | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H |

| Proprietary Code CVEs | Description | CVSS Base Score | CVSS Vector String |
|---|---|---|---|
| CVE-2026-23779 | Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.50, contain a command injection vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability to gain root-level access. | 6.7 | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H |
| CVE-2026-35153 | Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7.0.0, LTS2025 release versions 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60 contain an improper neutralization of argument delimiters in a command ('argument injection') vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges. | 6.7 | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H |
| CVE-2026-35072 | Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7.0.0, LTS2025 release versions 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60 contain 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 arbitrary command execution with root privileges. | 6.7 | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H |
| CVE-2026-35074 | Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7.0.0, LTS2025 release versions 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60 contain an improper neutralization of special elements used in an OS Command Injection vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges. | 6.7 | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H |
| CVE-2026-35073 | Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7.0.0, LTS2025 release versions 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60 contain an improper neutralization of special elements used in an OS command injection vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges. | 6.7 | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H |
| CVE-2025-46607 | Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 8.4 through 8.5 contain an improper authentication vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access. | 6.6 | CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H |

| Proprietary Code CVEs | Description | CVSS Base Score | CVSS Vector String |
|---|---|---|---|
| CVE-2025-46641 | Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 8.4 through 8.5 contain an improper authentication vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access. | 6.6 | CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H |
| CVE-2026-35154 | Dell PowerProtect Data Domain appliances, versions 7.7.1.0 through 8.7.0.0, LTS2025 release versions 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60 contain an improper privilege management vulnerability in IDRAC. A high privileged attacker with local access could potentially exploit this vulnerability, leading to elevation of privileges to access unauthorized delete operation in IDRAC. | 6.3 | CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H |
| CVE-2025-46605 | Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 8.4 through 8.5 contain a session fixation vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access. | 6.2 | CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:L |
| CVE-2025-46606 | Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 8.4 through 8.5 contain an improper restriction of excessive authentication attempts vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access. | 6.2 | CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:L |
| CVE-2026-28263 | Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.50, contain a cross-site Scripting vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Script injection. | 5.9 | CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:L |
| CVE-2026-23777 | Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.50, contain an exposure of sensitive information to an unauthorized actor vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to information exposure. | 4.3 | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N |

⚠ Dell Technologies recommends all customers consider both the CVSS base score and any relevant temporal and environmental scores that may impact the potential severity associated with a particular security vulnerability.

## Affected Products & Remediation

| CVEs Addressed | Product | Software/Firmware | Affected Versions | Remediated Versions | Link |
|---|---|---|---|---|---|
| CVE-2026-24504, CVE-2026-24506, CVE-2026-26943, CVE-2026-26942, CVE-2026-22761 | DD OS 8.6 | Dell PowerProtect Data Domain series appliances, Data Domain Virtual Edition, Dell APEX Protection Storage, and Data Domain Management Center with Data Domain Operating System (DD OS) Feature Release | Versions 7.7.1.0 through 8.6.0.0 | Versions 8.6.1.10, 8.7.0.0 or later | Data Domain Download |
| CVE-2026-35153, CVE-2026-35074 | DD OS 8.7 | Dell PowerProtect Data Domain series appliances, Data Domain Virtual Edition, Dell APEX Protection Storage, and Data Domain Management Center with Data Domain Operating System (DD OS) Feature Release | Versions 7.7.1.0 through 8.7.0.0 | Versions 8.6.1.10, 8.7.0.1 or later | Data Domain Download |
| CVE-2026-24504, CVE-2026-24506, CVE-2026-26943, CVE-2026-35153, CVE-2026-35074, CVE-2026-23776 | DD OS 8.3.1 | Dell PowerProtect Data Domain series appliances, Data Domain Virtual Edition, Dell APEX Protection Storage, and Data Domain Management Center with Data Domain Operating System (DD OS) LTS2025 8.3.1 | Versions 8.3.1.0 through 8.3.1.20 | Version 8.3.1.30 or later | Data Domain Download |
| CVE-2026-24504, CVE-2026-24506, CVE-2026-26943, CVE-2026-35153, CVE-2026-35074, CVE-2026-23776 | DD OS 7.13.1 | Dell PowerProtect Data Domain series appliances, Data Domain Virtual Edition, Dell APEX Protection Storage, and Data Domain Management Center with Data Domain Operating System (DD OS) LTS2024 7.13.1 | Versions 7.13.1.0 through 7.13.1.60 | Version 7.13.1.70 or later | Data Domain Download |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2026-26944, CVE-2026-24505, CVE-2026-26951, CVE-2026-26354 | DD OS 8.6 | Dell PowerProtect Data Domain series appliances, Data Domain Virtual Edition, and Dell APEX Protection Storage with Data Domain Operating System (DD OS) Feature Release | Versions 7.7.1.0 through 8.6.0.0 | Versions 8.6.1.10, 8.7.0.0 or later | Data Domain Download |
| CVE-2026-26354 | DD OS 8.3.1 | Dell PowerProtect Data Domain series appliances, Data Domain Virtual Edition, and Dell APEX Protection Storage with Data Domain Operating System (DD OS) LTS2025 8.3.1 | Versions 8.3.1.0 through 8.3.1.10 | Version 8.3.1.20 or later | Data Domain Download |
| CVE-2026-26354 | DD OS 7.13.1 | Dell PowerProtect Data Domain series appliances, Data Domain Virtual Edition, and Dell APEX Protection Storage with Data Domain Operating System (DD OS) LTS2024 7.13.1 | Versions 7.13.1.0 through 7.13.1.50 | Version 7.13.1.60 or later | Data Domain Download |
| CVE-2026-35072 | DD OS 8.7 | Dell PowerProtect Data Domain series appliances, Data Domain Virtual Edition, and Dell APEX Protection Storage with Data Domain Operating System (DD OS) Feature Release | Versions 7.7.1.0 through 8.7.0.0 | Versions 8.6.1.10, 8.7.0.1 or later | Data Domain Download |
| CVE-2026-26944, CVE-2026-26951, CVE-2026-35072 | DD OS 8.3.1 | Dell PowerProtect Data Domain series appliances, Data Domain Virtual Edition, and Dell APEX Protection Storage with Data Domain Operating System (DD OS) LTS2025 8.3.1 | Versions 8.3.1.0 through 8.3.1.20 | Version 8.3.1.30 or later | Data Domain Download |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2026-26944, CVE-2026-26951, CVE-2026-35072 | DD OS 7.13.1 | Dell PowerProtect Data Domain series appliances, Data Domain Virtual Edition, and Dell APEX Protection Storage with Data Domain Operating System (DD OS) LTS2024 7.13.1 | Versions 7.13.1.0 through 7.13.1.60 | Version 7.13.1.70 or later | Data Domain Download |
| CVE-2026-23775 | DD OS 8.5 | Dell PowerProtect Data Domain series appliances with Data Domain Operating System (DD OS) Feature Release | Versions 8.3.0.0 through 8.5.0.0 | Version 8.6.0.0 or later | Data Domain Download |
| CVE-2026-23775 | DD OS 8.3.1 | Dell PowerProtect Data Domain series appliances with Data Domain Operating System (DD OS) LTS2025 8.3.1 | Versions 8.3.1.0 through 8.3.1.10 | Version 8.3.1.20 or later | Data Domain Download |
| CVE-2026-35073, CVE-2026-35154 | DD OS 8.7 | Dell PowerProtect Data Domain series appliances with Data Domain Operating System (DD OS) Feature Release | Versions 8.3.0.0 through 8.7.0.0 | Versions 8.6.1.10, 8.7.0.1 or later | Data Domain Download |
| CVE-2026-35073, CVE-2026-35154 | DD OS 8.3.1 | Dell PowerProtect Data Domain series appliances with Data Domain Operating System (DD OS) LTS2025 8.3.1 | Versions 8.3.1.0 through 8.3.1.20 | Version 8.3.1.30 or later | Data Domain Download |
| CVE-2026-35073, CVE-2026-35154 | DD OS 7.13.1 | Dell PowerProtect Data Domain series appliances with Data Domain Operating System (DD OS) LTS2024 7.13.1 | Versions 7.13.1.0 through 7.13.1.60 | Version 7.13.1.70 or later | Data Domain Download |
| CVE-2025-46605, CVE-2025-46606, CVE-2025-46607, CVE-2025-46641 | DD OS 8.5 | Dell PowerProtect Data Domain series appliances, Data Domain Virtual Edition, and Dell APEX Protection Storage with Data Domain Operating System (DD OS) Feature Release | Versions 8.4.0.0 through 8.5.0.0 | Version 8.6.0.0 or later | Data Domain Download |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2025-48976, CVE-2025-37925, CVE-2025-37805, CVE-2025-37803, CVE-2025-37802, CVE-2025-37801, CVE-2025-37800, CVE-2025-37785, CVE-2025-23136, CVE-2025-22063, CVE-2025-22038, CVE-2025-22037, CVE-2025-22027, CVE-2025-22018, CVE-2025-22007, CVE-2025-21996, CVE-2025-21993, CVE-2024-9143, CVE-2026-23853, CVE-2026-23778, CVE-2026-23776, CVE-2026-23779, CVE-2026-28263, CVE-2026-23777, CVE-2026-23774 | DD OS 8.5 | Dell PowerProtect Data Domain series appliances, Data Domain Virtual Edition, Dell APEX Protection Storage, and Data Domain Management Center with Data Domain Operating System (DD OS) Feature Release | Versions 7.7.1.0 through 8.5.0.0 | Version 8.6.0.0 or later | Data Domain Download |
| CVE-2025-48976, CVE-2025-37925, CVE-2025-37805, CVE-2025-37803, CVE-2025-37802, CVE-2025-37801, CVE-2025-37800, CVE-2025-37785, CVE-2025-23136, CVE-2025-22063, CVE-2025-22038, CVE-2025-22037, CVE-2025-22027, CVE-2025-22018, CVE-2025-22007, CVE-2025-21996, CVE-2025-21993, CVE-2024-9143, CVE-2026-23853, CVE-2026-23778, CVE-2026-23779, CVE-2026-28263, CVE-2026-23777, CVE-2026-23774 | DD OS 8.3.1 | Dell PowerProtect Data Domain series appliances, Data Domain Virtual Edition, Dell APEX Protection Storage, and Data Domain Management Center with Data Domain Operating System (DD OS) LTS2025 8.3.1 | Versions 8.3.1.0 through 8.3.1.10 | Version 8.3.1.20 or later | Data Domain Download |
| CVE-2025-48976, CVE-2025-37925, CVE-2025-37805, CVE-2025-37803, CVE-2025-37802, CVE-2025-37801, CVE-2025-37800, CVE-2025-37785, CVE-2025-23136, CVE-2025-22063, CVE-2025-22038, CVE-2025-22037, CVE-2025-22027, CVE-2025-22018, CVE-2025-22007, CVE-2025-21996, CVE-2025-21993, CVE-2024-9143, CVE-2026-23853, CVE-2026-23778, CVE-2026-23779, CVE-2026-28263, CVE-2026-23777, CVE-2026-23774 | DD OS 7.13.1 | Dell PowerProtect Data Domain series appliances, Data Domain Virtual Edition, Dell APEX Protection Storage, and Data Domain Management Center with Data Domain Operating System (DD OS) LTS2024 7.13.1 | Versions 7.13.1.0 through 7.13.1.40 | Version 7.13.1.50 or later | Data Domain Download |
| CVE-2016-9840, CVE-2025-5278, CVE-2024-2236, CVE-2025-4207, CVE-2024-12718, CVE-2025-0938, CVE-2025-4516, CVE-2025-6069, CVE-2025-6965, CVE-2025-4877, CVE-2025-4878,CVE-2025-5372, CVE-2025-5318, CVE-2025-4598, CVE-2025-6020, CVE-2024-47081, CVE-2025-49794, CVE-2025-49796, CVE-2025-7425, CVE-2025-6021, CVE-2025-6170 | DD OS 8.5 | Dell PowerProtect Data Domain Management Center with Data Domain Operating System (DD OS) Feature Release | Versions 7.7.1.0 through 8.5.0.0 | Version 8.6.0.0 or later | Data Domain Download |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2016-9840, CVE-2025-5278, CVE-2024-2236, CVE-2025-4207, CVE-2024-12718, CVE-2025-0938, CVE-2025-4516, CVE-2025-6069, CVE-2025-6965, CVE-2025-4877, CVE-2025-4878,CVE-2025-5372, CVE-2025-5318, CVE-2025-4598, CVE-2025-6020, CVE-2024-47081, CVE-2025-49794, CVE-2025-49796, CVE-2025-7425, CVE-2025-6021, CVE-2025-6170 | DD OS 8.3.1 | Dell PowerProtect Data Domain Management Center with Data Domain Operating System (DD OS) LTS2025 8.3.1 | Versions 8.3.1.0 through 8.3.1.20 | Version 8.3.1.30 or later | Data Domain Download |
| CVE-2016-9840, CVE-2025-5278, CVE-2024-2236, CVE-2025-4207, CVE-2024-12718, CVE-2025-0938, CVE-2025-4516, CVE-2025-6069, CVE-2025-6965, CVE-2025-4877, CVE-2025-4878,CVE-2025-5372, CVE-2025-5318, CVE-2025-4598, CVE-2025-6020, CVE-2024-47081, CVE-2025-49794, CVE-2025-49796, CVE-2025-7425, CVE-2025-6021, CVE-2025-6170 | DD OS 7.13.1 | Dell PowerProtect Data Domain Management Center with Data Domain Operating System (DD OS) LTS2024 7.13.1 | Versions 7.13.1.0 through 7.13.1.50 | Version 7.13.1.60 or later | Data Domain Download |
| CVE-2025-36568 | DD OS 8.5 | Dell PowerProtect Data Domain boostFS client with Data Domain Operating System (DD OS) Feature Release | Versions 7.7.1.0 through 8.5.0.0 | Version 8.6.0.0 or later | Data Domain Download |
| CVE-2025-36568 | DD OS 8.3.1 | Dell PowerProtect Data Domain boostFS client with Data Domain Operating System (DD OS) LTS2025 8.3.1 | Versions 8.3.1.0 through 8.3.1.20 | Version 8.3.1.30 or later | Data Domain Download |
| CVE-2025-36568 | DD OS 7.13.1 | Dell PowerProtect Data Domain boostFS client with Data Domain Operating System (DD OS) LTS2024 7.13.1 | Versions 7.13.1.0 through 7.13.1.50 | Version 7.13.1.60 or later | Data Domain Download |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2025-48976, CVE-2025-37925, CVE-2025-37805, CVE-2025-37803, CVE-2025-37802, CVE-2025-37801, CVE-2025-37800, CVE-2025-37785, CVE-2025-23136, CVE-2025-22063, CVE-2025-22038, CVE-2025-22037, CVE-2025-22027, CVE-2025-22018, CVE-2025-22007, CVE-2025-21996, CVE-2025-21993, CVE-2024-9143, CVE-2026-26944, CVE-2026-23853, CVE-2026-23774, CVE-2026-24504, CVE-2026-24505, CVE-2026-24506, CVE-2026-26943, CVE-2026-23778, CVE-2026-23776, CVE-2026-26942, CVE-2026-22761, CVE-2026-26951, CVE-2026-23779, CVE-2026-35153, CVE-2026-35072, CVE-2026-35074, CVE-2026-28263, CVE-2026-23777, CVE-2026-26354 | PowerProtect DP Series Appliance (IDPA) | PowerProtect DP Series Software | Versions prior to 2.7.9 | Version 2.7.9 with DD OS 8.3.1.30 | Data Domain Download |

| CVEs Addressed | Product | Software/Firmware | Affected Versions | Remediated Versions | Link |
|---|---|---|---|---|---|
| CVE-2026-24504, CVE-2026-24506, CVE-2026-26943, CVE-2026-26942, CVE-2026-22761 | DD OS 8.6 | Dell PowerProtect Data Domain series appliances, Data Domain Virtual Edition, Dell APEX Protection Storage, and Data Domain Management Center with Data Domain Operating System (DD OS) Feature Release | Versions 7.7.1.0 through 8.6.0.0 | Versions 8.6.1.10, 8.7.0.0 or later | Data Domain Download |
| CVE-2026-35153, CVE-2026-35074 | DD OS 8.7 | Dell PowerProtect Data Domain series appliances, Data Domain Virtual Edition, Dell APEX Protection Storage, and Data Domain Management Center with Data Domain Operating System (DD OS) Feature Release | Versions 7.7.1.0 through 8.7.0.0 | Versions 8.6.1.10, 8.7.0.1 or later | Data Domain Download |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2026-24504, CVE-2026-24506, CVE-2026-26943, CVE-2026-35153, CVE-2026-35074, CVE-2026-23776 | DD OS 8.3.1 | Dell PowerProtect Data Domain series appliances, Data Domain Virtual Edition, Dell APEX Protection Storage, and Data Domain Management Center with Data Domain Operating System (DD OS) LTS2025 8.3.1 | Versions 8.3.1.0 through 8.3.1.20 | Version 8.3.1.30 or later | Data Domain Download |
| CVE-2026-24504, CVE-2026-24506, CVE-2026-26943, CVE-2026-35153, CVE-2026-35074, CVE-2026-23776 | DD OS 7.13.1 | Dell PowerProtect Data Domain series appliances, Data Domain Virtual Edition, Dell APEX Protection Storage, and Data Domain Management Center with Data Domain Operating System (DD OS) LTS2024 7.13.1 | Versions 7.13.1.0 through 7.13.1.60 | Version 7.13.1.70 or later | Data Domain Download |
| CVE-2026-26944, CVE-2026-24505, CVE-2026-26951, CVE-2026-26354 | DD OS 8.6 | Dell PowerProtect Data Domain series appliances, Data Domain Virtual Edition, and Dell APEX Protection Storage with Data Domain Operating System (DD OS) Feature Release | Versions 7.7.1.0 through 8.6.0.0 | Versions 8.6.1.10, 8.7.0.0 or later | Data Domain Download |
| CVE-2026-26354 | DD OS 8.3.1 | Dell PowerProtect Data Domain series appliances, Data Domain Virtual Edition, and Dell APEX Protection Storage with Data Domain Operating System (DD OS) LTS2025 8.3.1 | Versions 8.3.1.0 through 8.3.1.10 | Version 8.3.1.20 or later | Data Domain Download |
| CVE-2026-26354 | DD OS 7.13.1 | Dell PowerProtect Data Domain series appliances, Data Domain Virtual Edition, and Dell APEX Protection Storage with Data Domain Operating System (DD OS) LTS2024 7.13.1 | Versions 7.13.1.0 through 7.13.1.50 | Version 7.13.1.60 or later | Data Domain Download |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2026-35072 | DD OS 8.7 | Dell PowerProtect Data Domain series appliances, Data Domain Virtual Edition, and Dell APEX Protection Storage with Data Domain Operating System (DD OS) Feature Release | Versions 7.7.1.0 through 8.7.0.0 | Versions 8.6.1.10, 8.7.0.1 or later | Data Domain Download |
| CVE-2026-26944, CVE-2026-26951, CVE-2026-35072 | DD OS 8.3.1 | Dell PowerProtect Data Domain series appliances, Data Domain Virtual Edition, and Dell APEX Protection Storage with Data Domain Operating System (DD OS) LTS2025 8.3.1 | Versions 8.3.1.0 through 8.3.1.20 | Version 8.3.1.30 or later | Data Domain Download |
| CVE-2026-26944, CVE-2026-26951, CVE-2026-35072 | DD OS 7.13.1 | Dell PowerProtect Data Domain series appliances, Data Domain Virtual Edition, and Dell APEX Protection Storage with Data Domain Operating System (DD OS) LTS2024 7.13.1 | Versions 7.13.1.0 through 7.13.1.60 | Version 7.13.1.70 or later | Data Domain Download |
| CVE-2026-23775 | DD OS 8.5 | Dell PowerProtect Data Domain series appliances with Data Domain Operating System (DD OS) Feature Release | Versions 8.3.0.0 through 8.5.0.0 | Version 8.6.0.0 or later | Data Domain Download |
| CVE-2026-23775 | DD OS 8.3.1 | Dell PowerProtect Data Domain series appliances with Data Domain Operating System (DD OS) LTS2025 8.3.1 | Versions 8.3.1.0 through 8.3.1.10 | Version 8.3.1.20 or later | Data Domain Download |
| CVE-2026-35073, CVE-2026-35154 | DD OS 8.7 | Dell PowerProtect Data Domain series appliances with Data Domain Operating System (DD OS) Feature Release | Versions 8.3.0.0 through 8.7.0.0 | Versions 8.6.1.10, 8.7.0.1 or later | Data Domain Download |
| CVE-2026-35073, CVE-2026-35154 | DD OS 8.3.1 | Dell PowerProtect Data Domain series appliances with Data Domain Operating System (DD OS) LTS2025 8.3.1 | Versions 8.3.1.0 through 8.3.1.20 | Version 8.3.1.30 or later | Data Domain Download |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2026-35073, CVE-2026-35154 | DD OS 7.13.1 | Dell PowerProtect Data Domain series appliances with Data Domain Operating System (DD OS) LTS2024 7.13.1 | Versions 7.13.1.0 through 7.13.1.60 | Version 7.13.1.70 or later | Data Domain Download |
| CVE-2025-46605, CVE-2025-46606, CVE-2025-46607, CVE-2025-46641 | DD OS 8.5 | Dell PowerProtect Data Domain series appliances, Data Domain Virtual Edition, and Dell APEX Protection Storage with Data Domain Operating System (DD OS) Feature Release | Versions 8.4.0.0 through 8.5.0.0 | Version 8.6.0.0 or later | Data Domain Download |
| CVE-2025-48976, CVE-2025-37925, CVE-2025-37805, CVE-2025-37803, CVE-2025-37802, CVE-2025-37801, CVE-2025-37800, CVE-2025-37785, CVE-2025-23136, CVE-2025-22063, CVE-2025-22038, CVE-2025-22037, CVE-2025-22027, CVE-2025-22018, CVE-2025-22007, CVE-2025-21996, CVE-2025-21993, CVE-2024-9143, CVE-2026-23853, CVE-2026-23778, CVE-2026-23776, CVE-2026-23779, CVE-2026-28263, CVE-2026-23777, CVE-2026-23774 | DD OS 8.5 | Dell PowerProtect Data Domain series appliances, Data Domain Virtual Edition, Dell APEX Protection Storage, and Data Domain Management Center with Data Domain Operating System (DD OS) Feature Release | Versions 7.7.1.0 through 8.5.0.0 | Version 8.6.0.0 or later | Data Domain Download |
| CVE-2025-48976, CVE-2025-37925, CVE-2025-37805, CVE-2025-37803, CVE-2025-37802, CVE-2025-37801, CVE-2025-37800, CVE-2025-37785, CVE-2025-23136, CVE-2025-22063, CVE-2025-22038, CVE-2025-22037, CVE-2025-22027, CVE-2025-22018, CVE-2025-22007, CVE-2025-21996, CVE-2025-21993, CVE-2024-9143, CVE-2026-23853, CVE-2026-23778, CVE-2026-23779, CVE-2026-28263, CVE-2026-23777, CVE-2026-23774 | DD OS 8.3.1 | Dell PowerProtect Data Domain series appliances, Data Domain Virtual Edition, Dell APEX Protection Storage, and Data Domain Management Center with Data Domain Operating System (DD OS) LTS2025 8.3.1 | Versions 8.3.1.0 through 8.3.1.10 | Version 8.3.1.20 or later | Data Domain Download |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2025-48976, CVE-2025-37925, CVE-2025-37805, CVE-2025-37803, CVE-2025-37802, CVE-2025-37801, CVE-2025-37800, CVE-2025-37785, CVE-2025-23136, CVE-2025-22063, CVE-2025-22038, CVE-2025-22037, CVE-2025-22027, CVE-2025-22018, CVE-2025-22007, CVE-2025-21996, CVE-2025-21993, CVE-2024-9143, CVE-2026-23853, CVE-2026-23778, CVE-2026-23779, CVE-2026-28263, CVE-2026-23777, CVE-2026-23774 | DD OS 7.13.1 | Dell PowerProtect Data Domain series appliances, Data Domain Virtual Edition, Dell APEX Protection Storage, and Data Domain Management Center with Data Domain Operating System (DD OS) LTS2024 7.13.1 | Versions 7.13.1.0 through 7.13.1.40 | Version 7.13.1.50 or later | Data Domain Download |
| CVE-2016-9840, CVE-2025-5278, CVE-2024-2236, CVE-2025-4207, CVE-2024-12718, CVE-2025-0938, CVE-2025-4516, CVE-2025-6069, CVE-2025-6965, CVE-2025-4877, CVE-2025-4878,CVE-2025-5372, CVE-2025-5318, CVE-2025-4598, CVE-2025-6020, CVE-2024-47081, CVE-2025-49794, CVE-2025-49796, CVE-2025-7425, CVE-2025-6021, CVE-2025-6170 | DD OS 8.5 | Dell PowerProtect Data Domain Management Center with Data Domain Operating System (DD OS) Feature Release | Versions 7.7.1.0 through 8.5.0.0 | Version 8.6.0.0 or later | Data Domain Download |
| CVE-2016-9840, CVE-2025-5278, CVE-2024-2236, CVE-2025-4207, CVE-2024-12718, CVE-2025-0938, CVE-2025-4516, CVE-2025-6069, CVE-2025-6965, CVE-2025-4877, CVE-2025-4878,CVE-2025-5372, CVE-2025-5318, CVE-2025-4598, CVE-2025-6020, CVE-2024-47081, CVE-2025-49794, CVE-2025-49796, CVE-2025-7425, CVE-2025-6021, CVE-2025-6170 | DD OS 8.3.1 | Dell PowerProtect Data Domain Management Center with Data Domain Operating System (DD OS) LTS2025 8.3.1 | Versions 8.3.1.0 through 8.3.1.20 | Version 8.3.1.30 or later | Data Domain Download |
| CVE-2016-9840, CVE-2025-5278, CVE-2024-2236, CVE-2025-4207, CVE-2024-12718, CVE-2025-0938, CVE-2025-4516, CVE-2025-6069, CVE-2025-6965, CVE-2025-4877, CVE-2025-4878,CVE-2025-5372, CVE-2025-5318, CVE-2025-4598, CVE-2025-6020, CVE-2024-47081, CVE-2025-49794, CVE-2025-49796, CVE-2025-7425, CVE-2025-6021, CVE-2025-6170 | DD OS 7.13.1 | Dell PowerProtect Data Domain Management Center with Data Domain Operating System (DD OS) LTS2024 7.13.1 | Versions 7.13.1.0 through 7.13.1.50 | Version 7.13.1.60 or later | Data Domain Download |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2025-36568 | DD OS 8.5 | Dell PowerProtect Data Domain boostFS client with Data Domain Operating System (DD OS) Feature Release | Versions 7.7.1.0 through 8.5.0.0 | Version 8.6.0.0 or later | Data Domain Download |
| CVE-2025-36568 | DD OS 8.3.1 | Dell PowerProtect Data Domain boostFS client with Data Domain Operating System (DD OS) LTS2025 8.3.1 | Versions 8.3.1.0 through 8.3.1.20 | Version 8.3.1.30 or later | Data Domain Download |
| CVE-2025-36568 | DD OS 7.13.1 | Dell PowerProtect Data Domain boostFS client with Data Domain Operating System (DD OS) LTS2024 7.13.1 | Versions 7.13.1.0 through 7.13.1.50 | Version 7.13.1.60 or later | Data Domain Download |
| CVE-2025-48976, CVE-2025-37925, CVE-2025-37805, CVE-2025-37803, CVE-2025-37802, CVE-2025-37801, CVE-2025-37800, CVE-2025-37785, CVE-2025-23136, CVE-2025-22063, CVE-2025-22038, CVE-2025-22037, CVE-2025-22027, CVE-2025-22018, CVE-2025-22007, CVE-2025-21996, CVE-2025-21993, CVE-2024-9143, CVE-2026-26944, CVE-2026-23853, CVE-2026-23774, CVE-2026-24504, CVE-2026-24505, CVE-2026-24506, CVE-2026-26943, CVE-2026-23778, CVE-2026-23776, CVE-2026-26942, CVE-2026-22761, CVE-2026-26951, CVE-2026-23779, CVE-2026-35153, CVE-2026-35072, CVE-2026-35074, CVE-2026-28263, CVE-2026-23777, CVE-2026-26354 | PowerProtect DP Series Appliance (IDPA) | PowerProtect DP Series Software | Versions prior to 2.7.9 | Version 2.7.9 with DD OS 8.3.1.30 | Data Domain Download |

**Note:**

1. PowerProtect Data Domain: Software Versions: This KB article provides the status of the current active PowerProtect Data Domain Operating System (DD OS) releases, along with links to the release notes. (Requires support.dell.com login to view article).
2. For instructions on how to upgrade Data Domain Operating System (DD OS), see Data Domain and DDVE: How to Upgrade the Data Domain Operating System
3. DD OS Version 8.6.1.10 is the first release of LTS 2026 and includes the fixes for all CVEs disclosed in this advisory.
4. Data Domain: iDRAC Operator User Changes in DDOS
5. Some security scanners may still report False Positive findings after upgrading to remediated DD OS versions. For more details, please refer to the respective False Positive KB articles:
   - Dell PowerProtect Data Domain False Positive Security Vulnerabilities for DD OS 8.7
   - Dell PowerProtect Data Domain False Positive Security Vulnerabilities for DD OS 8.6
   - Dell PowerProtect Data Domain False Positive Security Vulnerabilities for DD OS 8.3
   - Dell Data Domain False Positive Security Vulnerabilities for DD OS 7.13

## Revision History

| Revision | Date | Description |
|---|---|---|
| 1.0 | 2026-04-14 | Initial Release |
| 2.0 | 2026-04-15 | Updated for enhanced presentation with no changes to content |
| 3.0 | 2026-04-16 | Added PowerProtect Data Domain LTS 8.6.1.10 and additional details in notes section |
| 4.0 | 2026-04-16 | Updated for enhanced presentation with no changes to content |
| 5.0 | 2026-04-20 | Updated Additional Info section to include additional details for LTS 8.6.1.10, iDRAC Operator User Changes in DDOS KB Article, Added CVE-2026-26354 |

## Acknowledgements

- CVE-2026-23774, CVE-2026-24506: Dell would like to thank zzcentury from Ubisectech Sirius Team for reporting these issues.
- CVE-2026-24504, CVE-2026-24505, CVE-2026-26942, CVE-2026-22761, CVE-2026-26943, CVE-2026-26951, CVE-2026-26944: Dell would like to thank brocked200 (Nguyen Quoc Khanh) for reporting these issues.

## Related Information

Dell Security Advisories and Notices
Dell Vulnerability Response Policy
CVSS Scoring Guide

## Legal Disclaimer

## Affected Products

Data Domain, PowerProtect Data Protection Appliance, PowerProtect Data Manager Appliance, DD3300 Appliance, Data Domain Boost – File System, Data Domain Boost - Open Storage, Data Domain Deduplication Storage Systems, Data Domain Encryption ... View More

### Article Properties

**Article Number:** 000450699

**Article Type:** Dell Security Advisory

**Last Modified:** 21 Apr 2026

### Find answers to your questions from other Dell users

Visit Community

## Support Services

Check if your device is covered by Support Services.

Check Support Status