

# CVE-2021-21551

## Dell dbutil Driver Insufficient Access Control Vulnerability

CISA KEV since Mar 31, 2022

Actively exploited

Public exploit module (Metasploit)

Dell dbutil\_2\_3.sys driver contains an insufficient access control vulnerability which may lead to escalation of privileges, denial of service, or information disclosure. Local authenticated user access is required.

|                                                                     |                                              |                                                           |                                                                                    |
|---------------------------------------------------------------------|----------------------------------------------|-----------------------------------------------------------|------------------------------------------------------------------------------------|
| <b>EVRS</b><br><b>79</b> / <sub>100</sub><br><b>Urgent</b> priority | <b>CVSS V3.1</b><br><b>7.8</b><br>High · NVD | <b>EPSS</b><br><b>0.801</b><br>99.62nd percentile · FIRST | <b>CISA DEADLINE</b><br><b>Apr 21, 2022</b><br>KEV since 2022 · listed over a year |
|---------------------------------------------------------------------|----------------------------------------------|-----------------------------------------------------------|------------------------------------------------------------------------------------|

### Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

|                                                     |                                          |                                                                |                                            |
|-----------------------------------------------------|------------------------------------------|----------------------------------------------------------------|--------------------------------------------|
| <input checked="" type="checkbox"/> <b>CISA KEV</b> | Listed in the catalog                    | <input type="checkbox"/> <b>Vendor exploitation</b>            | Confirmed exploitation in the wild         |
| <input type="checkbox"/> <b>Ransomware</b>          | No known ransomware campaign association | <input type="checkbox"/> <b>KEV recency</b>                    | On the CISA KEV catalog for over two years |
| <input checked="" type="checkbox"/> <b>EPSS</b>     | 0.801 probability                        | <input type="checkbox"/> <b>Pre-patch disclosure</b>           | Disclosure status unavailable              |
| <input checked="" type="checkbox"/> <b>CVSS</b>     | Base score 7.8                           | <input type="checkbox"/> <b>Microsoft Exploitability Index</b> | Not a Microsoft CVE                        |

### Remediation

**Patch This Cycle** Patch or fixed version identified

**CISA required action:** Apply updates per vendor instructions.

Basis: CISA KEV required action

### Affected and fixed versions · 560 more affected products on the NVD record

| PACKAGE             | AFFECTED | FIXED IN                | SOURCE |
|---------------------|----------|-------------------------|--------|
| dbutil              | ≤ 2.3    | after 2.3               | NVD    |
| alienware 14        | —        | no fixed version listed | NVD    |
| alienware 17 51m r2 | —        | no fixed version listed | NVD    |
| alienware area 51   | —        | no fixed version listed | NVD    |
| alienware asm100    | —        | no fixed version listed | NVD    |
| alienware asm100r2  | —        | no fixed version listed | NVD    |
| alienware m14xr2    | —        | no fixed version listed | NVD    |
| alienware m15 r4    | —        | no fixed version listed | NVD    |

### Sources

**Vendor guidance** [github.com/advisories/GHSA-pp2j-9hqv-7x55](https://github.com/advisories/GHSA-pp2j-9hqv-7x55)

**Additional guidance** [dell.com/support/kbdoc/en-us/000186019/dsa-2021-088-dell-client-platform-security-update-for-dell-driver-insufficient-access-control-vulnerability](https://dell.com/support/kbdoc/en-us/000186019/dsa-2021-088-dell-client-platform-security-update-for-dell-driver-insufficient-access-control-vulnerability)  
**CISA KEV** [cisa.gov/known-exploited-vulnerabilities-catalog](https://cisa.gov/known-exploited-vulnerabilities-catalog)  
**Current data** [evulnable.com/vulnerability-management/cve/CVE-2021-21551](https://evulnable.com/vulnerability-management/cve/CVE-2021-21551)

**NVD** [nvd.nist.gov/vuln/detail/CVE-2021-21551](https://nvd.nist.gov/vuln/detail/CVE-2021-21551)

**ENISA EUVD** [euvd.enisa.europa.eu/vulnerability/EUVD-2021-8823](https://euvd.enisa.europa.eu/vulnerability/EUVD-2021-8823)

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.