**Cisco Talos odkrywa poważne podatności w ponad 100 modelach laptopów Dell**

Cisco Talos ujawnił pięć poważnych podatności w oprogramowaniu układowym **Dell ControlVault3** oraz w powiązanych z nim interfejsach API dla systemu Windows. Zbiorczo nazwane **ReVault**, luki te stanowią realne zagrożenie dla ponad 100 modeli laptopów Dell — często wykorzystywanych w środowiskach o podwyższonych wymaganiach bezpieczeństwa.

**Czym jest Dell ControlVault?**

[Dell ControlVault3](https://www.dell.com/support/home/en-vc/drivers/driversdetails?driverid=twf65) (oraz nowsza wersja ControlVault3+) to rozwiązanie sprzętowe odpowiedzialne za przechowywanie wrażliwych danych logowania: haseł, odcisków palców, szablonów biometrycznych czy kodów zabezpieczających. Zamiast przechowywać je w systemie operacyjnym, dane te trafiają do wydzielonego układu na płytce zwanej Unified Security Hub (USH), połączonej z czytnikiem linii papilarnych, kartą inteligentną czy modułem NFC.

Rozwiązanie to stosowane jest w ponad 100 modelach laptopów Dell – głównie z serii Latitude, Precision oraz Rugged – często wykorzystywanych w takich sektorach jak administracja publiczna, sektor finansowy czy infrastruktura krytyczna.

**Jak działa atak ReVault?**

ReVault to nie tylko zbiór luk w oprogramowaniu. To także potencjalny sposób na przejęcie pełnej kontroli nad komputerem – niezależnie od tego, czy napastnik działa zdalnie, czy ma fizyczny dostęp do urządzenia. Oto dwa możliwe scenariusze, które pokazują skalę ryzyka:

1. **Działania po przejęciu kontroli nad sprzętem**

W systemie Windows, nawet użytkownik bez uprawnień administratora może — za pomocą dostępnych API — nawiązać komunikację z firmware’em ControlVault i uruchomić w nim dowolny kod. Pozwala to m.in. na wykradanie kluczy kryptograficznych i trwałą modyfikację firmware’u. W efekcie możliwe jest zainstalowanie tzw. **implantu** — złośliwego kodu ukrytego w firmware, który może pozostać niewidoczny i zostać wykorzystany później do ponownego ataku, nawet po reinstalacji systemu.

1. **Atak fizyczny na sprzęt**

Wystarczy fizyczny dostęp do laptopa, by za pomocą złącza USB połączyć się z płytką USH (Unified Security Hub) i przeprowadzić atak — bez potrzeby znajomości hasła, PIN-u czy klucza szyfrowania dysku. Dodatkowo, jeśli system skonfigurowano do logowania odciskiem palca, zmodyfikowany firmware może zaakceptować dowolny odcisk, umożliwiając dostęp do systemu osobie nieuprawnionej.

**Jak ograniczyć ryzyko?**

* **Aktualizacja oprogramowania:**  
  Najskuteczniejszą metodą ochrony jest instalacja najnowszych wersji firmware’u. Dell udostępnia je najpierw na swojej stronie, a z czasem również przez Windows Update. **Dell udostępnił już aktualizacje, których instalacja rozwiązuje wykryty przez Cisco Talos problem. Można je** [**pobrać tutaj.**](https://www.dell.com/support/kbdoc/en-us/000276106/dsa-2025-053)
* **Wyłączenie nieużywanych komponentów:**  
  Jeśli urządzenia biometryczne (czytnik linii papilarnych, karta NFC, smart card) nie są wykorzystywane, warto wyłączyć odpowiednie usługi w Menedżerze usług i urządzeniach w Windows.
* **Zmiana ustawień logowania:**  
  W środowiskach podwyższonego ryzyka, takich jak hotele, przestrzenie współdzielone czy podróże służbowe, zaleca się tymczasowe wyłączenie logowania biometrycznego. Można także rozważyć aktywację funkcji Enhanced Sign-in Security (ESS) dostępnej w systemie Windows.

**Jak wykryć potencjalne naruszenie bezpieczeństwa?**

* **Detekcja fizycznej ingerencji:**  
  W wielu modelach laptopów Dell można w BIOS-ie włączyć detekcję otwarcia obudowy. System poinformuje użytkownika o możliwym naruszeniu fizycznym.
* **Monitorowanie logów systemowych:**  
  Nieoczekiwane awarie usług, takich jak Windows Biometric Service czy Credential Vault, mogą sugerować próbę ataku lub nieprawidłowe działanie firmware’u.
* **Sygnatury w oprogramowaniu ochronnym:**  
  Użytkownicy Cisco Secure Endpoint powinni zwrócić uwagę na alert: „bcmbipdll.dll Loaded by Abnormal Process”, który może wskazywać na nieautoryzowaną aktywność.

Incydent ReVault po raz kolejny udowadnia, że cyberbezpieczeństwo nie kończy się na systemie operacyjnym. Sprzęt, na którym działa system, powinien być traktowany jako równie istotny element bezpieczeństwa co oprogramowanie czy jego konfiguracja.

Podatności w firmware’ach, takich jak Dell ControlVault, pokazują, że nawet najlepiej zabezpieczone środowiska mogą zostać przełamane, jeśli jeden z komponentów zostanie pominięty w ocenie ryzyka. Prawdziwe bezpieczeństwo wymaga pełnej widoczności – od aplikacji, przez system, aż po warstwę sprzętową.

Więcej informacji na blogu Cisco Talos: <https://blog.talosintelligence.com/revault-when-your-soc-turns-against-you/>

.:|:.:|:.

**O Cisco**

Cisco (NASDAQ: CSCO) to światowy lider technologiczny, który rewolucjonizuje sposób, w jaki organizacje łączą się i chronią w erze AI. Od ponad 40 lat Cisco bezpiecznie łączy świat. Dzięki wiodącym w branży rozwiązaniom i usługom opartym na AI, Cisco umożliwia swoim klientom, partnerom i społecznościom odblokowanie innowacji, zwiększenie produktywności i wzmocnienie odporności cyfrowej oraz pozostaje zaangażowane w tworzenie bardziej połączonej i inkluzywnej przyszłości dla wszystkich.

Cisco i logo Cisco są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Cisco i/lub jej podmiotów stowarzyszonych w Stanach Zjednoczonych i innych krajach. Listę znaków towarowych Cisco można znaleźć na stronie www.cisco.com/go/trademarks. Wymienione znaki towarowe innych firm są własnością ich odpowiednich właścicieli. Użycie słowa partner nie oznacza relacji partnerskiej między Cisco a jakąkolwiek inną firmą.

Kontakt: Łukasz Dąbrowski | ldabrows@cisco.com | tel.: 795 03 12 02