Advisory Alert

Alert Number: AAA20240607 **Date:** June 7, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Solarwinds	**High**	Directory Transversal Vulnerability
WatchGuard	**High**	TunnelVision Vulnerability
Dell	**High**	Integrity Check Vulnerability

Description

Affected Product	**Solarwinds**
Severity	**High**
Affected Vulnerability	Directory Transversal Vulnerability (CVE-2024-28995)
Description	Solarwinds has released a security update addressing a directory transversal vulnerability that exists in their products. Exploitation of this vulnerability would allow access to read sensitive files on the host machine. Solarwinds advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SolarWinds Serv-U 15.4.2 HF 1 and previous versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.solarwinds.com/trust-center/security-advisories/cve-2024-28995

Affected Product	**WatchGuard**
Severity	**High**
Affected Vulnerability	TunnelVision Vulnerability (CVE-2024-3661)
Description	WatchGuard has released workarounds addressing the TunnelVision Vulnerability that affects WatchGuard Mobile VPN and WatchGuard IPSEC Mobile VPN Client. An attacker on the same local network can exploit this vulnerability to divert traffic out of the tunnel, allowing them to disrupt and potentially read or modify unencrypted connections. WatchGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	WatchGuard Mobile VPN with SSL for Windows - All Version(s) WatchGuard Mobile VPN with SSL for macOS - All Version(s) WatchGuard IPSEC Mobile VPN Client for Windows (NCP) - All Version(s) WatchGuard IPSEC Mobile VPN Client for macOS (NCP) - All Version(s)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2024-00009

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Integrity Check Vulnerability (CVE-2023-32475)
Description	Dell has released security updates addressing an Integrity Check Vulnerability that exists in Dell Client Platform AMD BIOS. This vulnerability could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Alienware Aurora R10 BIOS Versions prior to 2.6.0 Alienware Aurora R15 AMD BIOS Versions prior to 1.13.0 Alienware Aurora Ryzen Edition R14 BIOS Versions prior to 2.16.0 Alienware m15 R7 AMD BIOS Versions prior to 1.15.0 Alienware m15 Ryzen Edition R5 BIOS Versions prior to 1.16.0 Alienware m16 R1 AMD BIOS Versions prior to 1.9.0 Alienware m17 R5 AMD BIOS Versions prior to 1.15.0 Alienware m18 BIOS Versions prior to 1.9.0 Dell G15 5515 BIOS Versions prior to 1.15.0 Dell G15 5525 BIOS Versions prior to 1.15.0 Dell G15 5535 BIOS Versions prior to 1.5.0 Dell G5 5505 BIOS Versions prior to 1.18.0 Inspiron 14 5425 BIOS Versions prior to 1.13.0 Inspiron 14 5435 BIOS Versions prior to 1.8.0 Inspiron 14 7425 2-in-1 BIOS Versions prior to 1.13.0 Inspiron 14 7435 2-in-1 BIOS Versions prior to 1.8.0 Inspiron 15 3515 BIOS Versions prior to 1.16.0 Inspiron 15 3525 BIOS Versions prior to 1.15.1 Inspiron 15 3535 BIOS Versions prior to 1.12.0 Inspiron 16 5625 BIOS Versions prior to 1.13.0 Inspiron 16 5635 BIOS Versions prior to 1.8.0 Inspiron 16 7635 2-in-1 BIOS Versions prior to 1.8.0 Inspiron 24 5415 All-in-One BIOS Versions prior to 1.17.0 Inspiron 3505 BIOS Versions prior to 1.16.0 Inspiron 5405 BIOS Versions prior to 1.14.0 Inspiron 5415 BIOS Versions prior to 1.19.0 Inspiron 5505 BIOS Versions prior to 1.14.0 Inspiron 5515 BIOS Versions prior to 1.19.0 Inspiron 7405 2-in-1 BIOS Versions prior to 1.15.0 Inspiron 7415 2-in-1 BIOS Versions prior to 1.19.0 Vostro 14 3425 BIOS Versions prior to 1.15.1 Vostro 14 3435 BIOS Versions prior to 1.12.0 Vostro 15 3515 BIOS Versions prior to 1.16.0 Vostro 15 3525 BIOS Versions prior to 1.15.1 Vostro 15 3535 BIOS Versions prior to 1.12.0 Vostro 16 5635 BIOS Versions prior to 1.8.0 Vostro 3405 BIOS Versions prior to 1.16.0 Vostro 5415 BIOS Versions prior to 1.19.0 Vostro 5515 BIOS Versions prior to 1.19.0 Vostro 5625 BIOS Versions prior to 1.13.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000215644/dsa-2023-222-security-update-for-an-amd-bios-vulnerability

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.