مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerabilities in Dell Enterprise SONiC OS

Tracking #:432316497

Date:12-11-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Dell Technologies has issued a critical security advisory addressing multiple vulnerabilities within the Dell Enterprise SONiC OS, which could allow attackers to compromise affected systems.

TECHNICAL DETAILS:

Dell Technologies has issued a critical security advisory addressing multiple vulnerabilities within the Dell Enterprise SONiC OS, which could allow attackers to compromise affected systems. These vulnerabilities, identified as CVE-2024-45763, CVE-2024-45764, and CVE-2024-45765, affect versions 4.1.x and 4.2.x of the Enterprise SONiC operating system.

Vulnerability Details

CVE-2024-45763 – OS Command Injection

- **Description**: This vulnerability exists due to improper neutralization of special elements used in OS commands, allowing a high-privilege attacker with remote access to execute arbitrary commands on the affected system.
- **CVSS Base Score**: **9.1 (Critical)**
- **Impact**: Successful exploitation could result in full control over the affected system.

CVE-2024-45764 – Missing Critical Step in Authentication

- **Description**: A flaw in the authentication mechanism could allow unauthenticated attackers with remote access to bypass protection mechanisms, potentially leading to unauthorized access.
- **CVSS Base Score**: **9.0 (Critical)**
- **Impact**: Exploiting this vulnerability would allow an attacker to gain unauthorized access to the system, potentially leading to further compromise.

CVE-2024-45765 – OS Command Injection (Privilege Escalation)

- **Description**: Another OS Command Injection vulnerability, but in this case, it allows less privileged attackers to execute high-privilege OS commands, escalating their access to administrative-level control.
- **CVSS Base Score**: **9.1 (Critical)**
- **Impact**: An attacker with lower privileges could exploit this vulnerability to elevate their access and execute commands that could compromise the integrity of the system.

Fixed versions: Dell Enterprise SONiC OS version 4.1.6 or 4.2.2

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to install the fixed versions at the earliest.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.dell.com/support/kbdoc/en-us/000245655/dsa-2024-449-security-update-for-dell-enterprise-sonic-distribution-vulnerabilities