Severity

Medium

Analysis Summary

CVE-2022-1701 CVSS:5.7

SonicWall SMA1000 series could allow a local authenticated attacker to obtain sensitive information, caused by the use of a shared and hard-coded encryption key to store data. By sending a specially-crafted request, an attacker could exploit this vulnerability to obtain sensitive information, and use this information to launch further attacks against the affected system.

CVE-2022-1702 CVSS:6.1

SonicWall SMA1000 series could allow a remote attacker to conduct phishing attacks, caused by an open redirect vulnerability. An attacker could exploit this vulnerability using a specially-crafted URL to redirect a victim to arbitrary Web sites.

CVE-2022-22282 CVSS:8.2

SonicWall SMA1000 series could allow a remote attacker to bypass security restrictions, caused by improper access control. By sending a specially-crafted request, an attacker could exploit this vulnerability to bypass access restrictions.

Impact

- Information Disclosure
- Gain Access
- Security Bypass

Indicators Of Compromise

CVE

CVE-2022-1701

CVE-2022-1702

CVE-2022-22282

Affected Vendors

Sonicwall

Affected Products

- SonicWall SMA1000 series 12.4.0
- SonicWall SMA1000 series 12.4.1

Remediation

Refer to SonicWall Security Advisory for patch, upgrade or suggested workaround information.

SonicWall Security Advisor