**SSL Medium Strength Cipher Suites Supported (SWEET32)**

Medium strength encryption SSL ciphers can be used with the remote host. Any encryption that employs the 3DES encryption suite or key lengths of at least 64 bits but less than 112 bits is regarded by Nessus as medium strength.

**Exploit:** SSL/TLS configurations, disable the use of 64-bit block ciphers, especially Triple-DES. To give

stronger cipher suites priority, update the settings on your server. Set up server to use strong encryption cipher suites that are up to date and secure. Steer clear of old or inadequate ciphers.

**Mitigation**: We disable all 64-bit block weak ciphers in order to protect sensitive data from this serious SWEET32 birthday attack vulnerability. Strong ciphers like AES are the only ones we permit for increased security.Even though OpenSSL stopped supporting weak ciphers in version 1.1.0 and later releases, we have observed that many servers are still using vulnerable older versions.

**Link:** https://bobcares.com/blog/sweet32-birthday-attack-cve-2016-

2183/#:~:text=To%20mitigate%20the%20SWEET32%20Birthday%20attack%20%28CVE-2016- 2183%29%20vulnerability%2C,weak%20ciphers%20from%20all%20the%20public%20SSL-

based%20services.

**Samba Badlock Vulnerability**

Due to improper authentication level negotiation over Remote Procedure, the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols have a flaw known as Badlock that affects the version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host.Use RPC (call) channels. This vulnerability allows a client and a server hosting a SAM database to force an authentication downgrade.

**Exploit:** A significant security weakness in Samba's handling of specific security descriptors during the processing of DCE/RPC (Distributed Computing Environment/Remote Procedure Call) requests was found to be the Badlock vulnerability. This vulnerability could be used by an attacker to execute man-in-the- middle attacks and intercept private data.Following the disclosure of the vulnerability, a concerted effort was made to resolve it, and patches were made available for Samba versions that were impacted. To reduce the danger of exploitation, system administrators were strongly encouraged to implement the updates right away.

# Mitigation:

1. Make sure Samba is up to date on your system. Updates and patches are made available by the Samba team to fix vulnerabilities, such as badlock. Use the package manager in your distribution or the official Samba website to install the most recent patches.
2. Update to the most recent stable release of the Samba software on a regular basis. You will always have the most recent security updates and enhancements thanks to this.
3. Segmenting your network could help reduce the impact of future attacks. Divide your network's less secure areas from your essential systems.

**Link:** [https://www.trendmicro.com/en\_gb/research/22/b/the-samba-vulnerability-what-is-cve-](https://www.trendmicro.com/en_gb/research/22/b/the-samba-vulnerability-what-is-cve-2021-44142-and-how-to-fix-it.html) [2021-44142-and-how-to-fix-it.html](https://www.trendmicro.com/en_gb/research/22/b/the-samba-vulnerability-what-is-cve-2021-44142-and-how-to-fix-it.html)

**SMB Signing not required**

A security feature in Microsoft Windows operating systems called SMB (Server Message Block) signing aids in preserving the authenticity and integrity of SMB packets sent between networked devices. When SMB signing is enabled, both the sender and the recipient of SMB packets use a cryptographic signature to confirm the sender's identity and guarantee that no tampering has occurred with the data while it was in transit.

**Exploit:** Packet sniffing tools allow an attacker positioned on the same network segment to intercept unencrypted SMB traffic. Sensitive data, such as usernames, passwords, and data being transferred between systems, may be made public as a result. An attacker could potentially take control of a user's

session by intercepting and replaying authentication tokens in the absence of SMB signing. Unauthorized access to file shares or other network resources may result from this.

# Mitigation:

1. Make sure the most recent patches and updates are installed on every system connected to your network. Updated software plays a critical role in fixing security flaws.
2. To further improve the security of SMB communications, think about putting IPsec into place. SMB traffic can be encrypted using IPsec, adding an extra degree of security.
3. Set up firewalls to limit exposure and restrict access to SMB services. Block unused ports and only let necessary traffic reach your SMB servers.
4. Maintain a regular backup of important data and make sure your disaster recovery plan is strong. Having current backups can reduce data loss in the case of a security incident.

**Link**: https://[www.tenable.com/plugins/nessus/57608](http://www.tenable.com/plugins/nessus/57608)