Network Scout Vulnerability Report

Prepared for **ABC Company**
January 1, 2017

Scan Description

Secure Ideas' Scout service is a high-frequency vulnerability assessment solution designed to help organizations better detect, and manage regular changes in their security posture. Unlike an annual, or semi-annual penetration test, these assessments provide a high level pass of the target(s) to find those common vulnerabilities that may pose a significant risk to the organization. The frequent nature of these assessments allows many vulnerabilities to be detected and addressed on a regular basis.

This report includes the results of the Scout scan initiated on **January 1, 2018** for **ABC Company Group.** The scope of this scan was as follows:

- 10.10.0.225
- 10.10.0.222
- 10.10.0.224
- 10.10.0.227

Executive Summary

Secure Ideas performed a vulnerability assessment against external IP addresses selected by **ABC Company** . The assessment was performed on January 1, 2018 and results were then validated and analyzed by Secure Ideas staff members.

During this assessment, a new critical vulnerability has been discovered regarding the Microsoft Secure Channel (Schannel) security package. The associated patch should be applied as soon as possible, as this flaw allows for remote code execution.

Some findings from the November report still exist, such as the legacy VPN device and the vulnerability called Padding Oracle On Downgraded Legacy Encryption (POODLE). This attack takes advantage of a negotiation feature to force the use of SSL 3.0. This vulnerability could allow an attacker to perform man-in-the-middle attacks and decrypt traffic. As a result, the protocol has reached the end of its useful life and should be retired.

Testing also discovered an area of weakness resulting from untrusted or self-signed SSL certificates. While this is not directly exploitable, it will result in browser warnings to users. Many organizations advise employees to simply ignore the warnings, since they know the internal site is safe, but this can encourage dangerous browsing behavior. Employees accustomed to ignoring warnings on internal sites may be inclined to ignore warnings on public sites as well.

These findings are outlined in the report that follows. One new vulnerability was discovered with this scan, and one vulnerability has been remediated from the previous scan.

Details

- Critical: 1
- High: 1
- Medium: 1
- Low: 3

Findings

Critical

- ***Missing Critical Patches***

Many of the patches released by application vendors are built to fix security issues found within the software. By not applying these patches, systems are exposed to attacks from malicious users or external attackers. Unpatched software currently in use could put the company at risk for man-in-the-middle attacks, denial of service issues, and remote code execution.

IP Address	Description	Recommendations
x.x.x.x	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611)	Microsoft has released a set of patches for Windows 2003, Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, and 2012 R2.

The remote Windows host is affected by a remote code execution vulnerability due to improper processing of packets by the Secure Channel (Schannel) security package. An attacker can exploit this issue by sending specially crafted packets to a Windows server.

Note that Secure Ideas sends a client Certificate TLS handshake message followed by a CertificateVerify message. Some Windows hosts will close the connection upon receiving a client certificate for which it did not ask for with a CertificateRequest message. In this case, Secure Ideas cannot proceed to detect the vulnerability as the CertificateVerify message cannot be sent.

The following Microsoft link contains more information about the vulnerability and the patch download:

https://technet.microsoft.com/library/security/ms14-066

High

- ***Use of End of Life Products***

End of life products no longer receive updates, or patches to protect from security vulnerabilities, therefore creating an entry point into the system.

IP Address	Description	Recommendations
x.x.x.x	End of Life Device - Cisco VPN 3000 Concentrator	Making the necessary upgrades will considerably reduce vulnerabilities to the network.
Secure Ideas found that ABC Company has deployed a Cisco VPN 3000 Concentrator. The interface for this device is available to the Internet, increasing its risk. *Similar to outdated software, a product that is labeled end of life (EOL) by the vendor will no longer receive support, therefore continued use of such products greatly increase the security threats on the system.* *This product was marked End of Life on 08/31/12 as shown in the link below:* *http://www.cisco.com/c/en/us/products/collateral/security/vpn-3000-series-concentrators/prod_end-of-life_notice0900aecd805cd5a0.html*		

Medium

- ***Insecure Configuration***

Server configurations play a key role in the security of a web application. Failure to manage the proper configuration of servers can lead to a wide variety of security problems.

IP Address	Description	Recommendations
x.x.x.x	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	Disable SSLv3. Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.
The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode. A MitM attacker can decrypt a selected		

byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

Low

- ***Weak Encryption***

The use of weak encryption algorithms may result in the loss of sensitive data. Connections to the server should enforce strong encrypted channels to protect the data that is transmitted back and forth.

IP Address	Description	Recommendations
x.x.x.x	SSL RC4 Cipher Suites Supported	Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

This host supports the use of RC4 in one or more cipher suites.

The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g. HTTP cookies), and an attacker is able to obtain many (i.e. tens of millions) ciphertexts, the attacker may be able to derive the plaintext.
Here is the list of RC4 cipher suites supported by the server:

High Strength Ciphers (>= 112-bit key)

TLSv1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1

- ***Insecure Use of Certificates***

Certificates contain identity information that is verified by a third party that your computer trusts. By checking that the address in the certificate matches the address of the website, it is possible to verify that you are securely communicating with the website you intended, and not a third party (such as an attacker on your network). Using an untrusted certificate authority or self-signed certificates makes it difficult for the end user to know if the certificate is valid for the respected site. This has the effect of teaching users to just allow untrusted certificates when they see the warning, which is bad practice.

IP Address	Description	Recommendations
x.x.x.x	SSL Certificate Cannot Be Trusted	Purchase or generate a proper certificate for this service.

The server's X.509 certificate does not have a signature from a known public certificate authority. This situation can occur in three different ways, each of which results in a break in the chain below which certificates cannot be trusted.

First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that connect the top of the certificate chain to a known certificate authority.

Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

Third, the certificate chain may contain a signature that either didn't match the certificate's information, or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that is not supported or recognized.

x.x.x.x	SSL Self-Signed Certificate	Purchase or generate a proper certificate for this service.

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this service does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority. Enable Network Level Authentication (NLA) on the remote RDP server.