NATIONAL SECURITY AGENCY
CYBERSECURITY OPERATIONAL RISK NOTICE

NETWORK SECURITY DEVICES UTILIZING VULNERABLE WEAK SIGNATURE ALGORITHMS IN TLS

RISK

Internal analysis indicates deprecated signature algorithms are widely implemented in network devices across some government networks. This ORN is being published based on current threat intelligence stating that nation-state and sufficiently resourced actors are able to exploit the weak communications that have been observed. These weak communication algorithms are vulnerable to numerous adversarial attacks such as man-in-the-middle attacks and certificate forgery. Unlike active exploits against devices, operating systems or application software, cryptographic exploits can be conducted passively from network locations that might not be monitored, or conducted in ways that leave no indication of the exploit. This allows the adversary to reduce the risk of detection or reprisal, and provides continued access to sensitive information. Researchers publish techniques, including code, which can be used or enhanced by less skilled adversaries to acquire exploitation capabilities.

Configuring network security devices to use weak signature algorithms allows malicious actors to defeat the device's intended security services and modify traffic to or from the device to inject additional malicious content via man-in-the-middle exploits. Man-in-the-middle exploits enabled by the use of weak signature algorithms also expose sensitive data in that traffic.

Certificates are installed to support digital signatures in network devices. Using weak signature algorithms allows an adversary to forge these certificates. Since the certificates are trusted by the systems being protected, an adversary can use the certificates in unintended ways to exploit the systems. Depending on the attributes of the forged certificates, an adversary could also impersonate users within the system, sign malicious updates to applications or operating systems, or sign malicious executables. Therefore, the risk is extremely high that nation states or other adequately skilled actors will gain undetected, persistent access, and potentially complete control of a system that trusts certificates with weak signature algorithms.

VULNERABILITY DISCUSSION

Network security devices, such as wireless access points, TLS proxies, security management systems, and web servers, use digital signatures so systems can discern that the devices are authentic, network traffic has been processed by the device, and traffic has not been modified in transit between the device and the system (via a man-in-the-middle exploit). Configuring network security devices to use deprecated signature algorithms or to use insufficient key sizes allows sufficiently resourced actors to forge signatures.

While large commercial certification authorities and managed, enterprise scale certification authorities will update certificates to use recommended signature algorithms, smaller or locally managed certification authorities may not. Also, some devices can generate individual self-signed certificates during installation. It is up to the administrator of these devices to update such certificates – a task that often goes overlooked. For example, an emerging trend is to deploy proxy servers, anti-virus software, and network security devices that claim to inspect encrypted data (SSL/TLS decryption). These security products contain embedded certification authorities that need to be properly configured and maintained. In all cases, the certificates issued on a device's embedded certification authority are widely trusted by the systems they are intended to protect. If the certificate in a security device uses weak signature algorithms, the vulnerability significantly increases the risk that the systems the products are intended to protect can be exploited.

VULNERABILITY DETECTION ACTIONS

Review the configuration of security devices and configure them to use the signature algorithms recommended by NIST SP 800-131[3]. National Security Systems are required to use algorithms and key sizes specified in CNSS-P 15[5]. Monitor network traffic and analyze logs of network devices for indicators of weak certificates, unexpected traffic, or other anomalous behavior that might indicate an exploit.

MITIGATION ACTIONS

It is NSA's position that these recommendations be implemented immediately. Delay in taking action related to this ORN could cause significant damage to the defense of customer and partner networks.

- Examine the configuration of network security devices, and ensure that they are configured to use approved algorithms[3,5], especially the signature algorithms used in certificates. Use NIAP validated products (see www.niap-ccevs.org/Product/) whenever possible and follow the vendor's configuration guide to ensure the product is configured as validated.
- Use certificates issued from well managed certificate authorities rather than self-signed certificates (TLS inspection products should use an enterprise certification authority specifically authorized for network defense operations rather than a publicly trusted certification authority). Ensure these certificates are properly configured, updated regularly and are revoked if there is an indication of possible compromise. If self-signed certificates must be used, ensure they are of short validity and are updated regularly with certificates that adhere to current cryptographic guidance.
- Manage operating system and browser trust stores to ensure all trusted certificates use recommended algorithms. Remove or 'un-trust' outdated or unnecessary certificates, especially those that were previously installed by users/administrators. This mitigation limits adversaries from exploiting trusted certificates for unanticipated consequences.

REMEDIATION REQUIREMENTS & ADVISORIES

[1] NIST SP 800-52 R1 "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations" http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf

[2] NIST SP 800-57 "Recommendation for Key Management –Part 1: General http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf

[3] NIST SP 800-131 R1 "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Length." http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf

[4] CNSS-P 25 "National Policy for Public Key Infrastructure in National Security Systems" https://www.cnss.gov/CNSS/issuances/Policies.cfm

[5] CNSS-P 15 "Use of Public Standards for Secure Information Sharing" https://www.cnss.gov/CNSS/issuances/Policies.cfm

[6] DoD-I 8520.02 "Public Key Infrastructure (PKI) and Public Key (PK) Enabling" http://www.dtic.mil/docs/citations/ADA573958

[7] "IA Hardening Authentication Guide" https://www.iad.gov/iad/library/ia-guidance/security-tips/Hardening-Authentication.cfm

DISCLAIMER OF WARRANTIES AND ENDORSEMENT

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

CONTACT INFORMATION

Client Requirements and Inquiries

Cybersecurity Requirements Center
410-854-4200
Cybersecurity_Requests@nsa.gov