Press release

February 7, 2025
National Center of Incident Readiness and Strategy for Cybersecurity

Co-sealing the Australian-Led International document on the Mitigation strategies for edge devices

1. Overview

On February 4, 2025, the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) co-sealed and published an international document entitled "Mitigation strategies for edge devices" (hereinafter referred to as the "Document"). The Document was authored by the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC). Tentative translations will be released as soon as possible.

The following countries co-sealed the Document and are listed in the Document: Australia, Japan, United States of America(US), United Kingdom (UK), Canada, New Zealand, South Korea, Netherlands and Czech Republic.

This document provides seven strategies for risk mitigation in light of the increasing number of attacks targeting edge devices by a number of malicious actors. The NISC co-sealed the Document because it will greatly contribute to the enhancement of Japan's cyber security if Japanese companies, including critical infrastructure providers, refer to the risk mitigation measures for edge devices described in this document.

The NISC will continue to make its efforts to foster international collaboration in the field of cybersecurity.

2. Overview of the Document

(1) Background and objectives

Many malicious actors conduct scanning and reconnaissance against internet-accessible networks to find unpatched software and exploit vulnerable devices. This Document provides a list of principle mitigation strategies for edge devices to improve security and resilience against cyber threats.

(2) Abstract of the seven strategies:

A) Know the Edge

Endeavour to understand where the periphery of the network is, and audit which devices sit across that edge. Identify devices that have reached End-of-Life (EOL) and remove/replace them

B) Procure secure-by-design devices

Prioritise procuring edge devices from manufacturers that follow secure-by-design principles during product development. Explicitly demand product security as part of the procurement process

C) Apply hardening guidance, updates and patches

Review and implement specific vendor hardening security guidance. Ensure prompt application of patches and updates to edge devices to protect against known vulnerabilities

D) Implement strong authentication
Implement phishing-resistant multifactor authentication (MFA) across edge devices to protect against exploitation.

E) Disable unneeded services and ports
Conduct an audit and disable any features that are being enabled by default and not being used by organisations to reduce the attack surface of the devices. Reduce the number of open ports.

F) Secure management interfaces
Limit exposure by ensuring management interfaces are not directly internet accessible

G) Centralise monitoring for threat detection
Ensure centralised visibility and log access to detect and investigate security incidents. Event logs should also be backed up and data redundancy practices should be implemented.

(End)