JPCERT Coordination Center

JPCERT/CC Activities Overview

October 1, 2020 ～ December 31, 2020

JPCERT Coordination Center

January 21, 2021

Activity Overview Topics

—Topic 1— Addressing vulnerabilities in VPN products as organizations increasingly adopt them to support remote work

Since April 2020, organizations have been making increasing use of VPN systems as part of their effort to combat COVID-19, and their importance has been increasing. Meanwhile, multiple products with SSL-VPN functionality have been used in considerable numbers without having known vulnerabilities fixed between 2019 and 2020, and actual damages have been reported as a result of attacks targeting those vulnerabilities. Amid this situation, JPCERT/CC has been taking additional measures after publishing vulnerability information and issuing security alerts, such as sending individual notices to the administrator of each device.

As part of these efforts, JPCERT/CC responded to a vulnerability in the SSL-VPN functionality of Fortinet's FortiOS this quarter. This vulnerability was published in May 2019, and JPCERT/CC issued a security alert in September 2019. This quarter, however, many systems were still operating without addressing the vulnerability even though more than a year has passed. In November 2020, a list of those systems was published on forums and elsewhere. This list was apparently prepared by attackers after checking that the vulnerability can be exploited, and in addition to the hosts' IP addresses, it contained user account names and plaintext passwords needed to use SSL-VPN connections. JPCERT/CC responded to this situation by issuing an alert to the general public through CyberNewsFlash, and it also provided information to organizations in Japan included in the list, either directly or through an ISP, a vendor, or other related organization, and requested that the situation be addressed immediately.

The spread of COVID-19 has triggered a major shift to a work style centered on remote work, and it is expected that VPN and other systems that connect via the Internet will increase going forward. To enhance measures against attacks seeking to exploit these circumstances, JPCERT/CC will publish a notice summarizing matters that require attention at the end of each quarter, in addition to relevant attack trends, together with information that has already been published and alerted on as well.

—Topic 2— JPCERT/CC activities aimed at establishing a global distribution platform for vulnerability information and addition of new CNAs from Japan

CVE Numbering Authorities (CNAs) assign Common Vulnerabilities and Exposures (CVE) identifiers, which are indispensable to the identification of vulnerability information. Originally, MITRE of the United States was the only CNA, but currently a number of CNAs are authorized to assign CVE IDs in a distributed fashion to be able to respond to the increasing amount of vulnerability information. A CNA that manages

other CNAs and performs necessary coordination is called a "Root CNA," and currently MITRE, JPCERT/CC and the CISA in the United States government serve as Root CNAs.

JPCERT/CC started operating as a CNA immediately after the launch of the multi-CNA system, and since 2018 when Root CNAs were established, it has worked together with MITRE to establish and promote the framework of CNAs. It has also cooperated with efforts to create Japanese translations of training materials for organizations that newly become a CNA, with the aim of establishing a distributed CVE numbering system comprising multiple CNAs within Japan.

These activities bore fruit on December 4, 2020, when LINE Corporation and Mitsubishi Electric Corporation were registered as the first CNAs with JPCERT/CC as the Root CNA.

JPCERT/CC Eyes "CNA activity report - 2 organizations from Japan newly added as CNAs"
https://blogs.jpcert.or.jp/en/2020/12/cna-2cna.html

Currently, there are 152 organizations registered as CNAs around the world, and it is expected that more Japanese organizations will be registered as CNAs. JPCERT/CC will aim to achieve even more rapid and effective distribution of vulnerability information and strive to establish collaborative relationships and systems with CNAs both in Japan and abroad.