AhnLab and NCSC Release Joint Report on Microsoft Zero-Day Browser Vulnerability (CVE-2024-38178)

A asec.ahnlab.com/en/83877/

October 15, 2024

AhnLab SEcurity intelligence Center (ASEC) and the National Cyber Security Center (NCSC) have discovered a new zero-day vulnerability in the Microsoft Internet Explorer (IE) browser and have conducted a detailed analysis on attacks that exploit this vulnerability. This post shares the joint analysis report "Operation Code on Toast by TA-RedAnt" which details the findings of the ASEC and NCSC joint analysis and the responses to the threat.

The North Korean threat actor TA-RedAnt (also known as RedEyes, ScarCruft, Group123, APT37, etc.) is behind this operation. They have previously targeted specific individuals such as North Korean defectors and experts in North Korean affairs using hacking emails, Android app package file (.apk), and IE vulnerabilities.

This operation exploited a zero-day vulnerability in IE to utilize a specific toast ad program that is installed alongside various free software.

※ Toast: A type of popup notification that appears at the bottom (usually right bottom) of the desktop screen.

Many toast ad programs use a feature called WebView to render web content for displaying ads. However, WebView operates based on a browser. Therefore, if the program creator used IE-based WebView to write the code, IE vulnerabilities could also be exploited in the program. As a result, TA-RedAnt exploited the toast ad program that were using the vulnerable IE browser engine (jscript9.dll), which is no longer supported, as an initial access vector. Microsoft ended its support for IE in June 2022. However, attacks that target some Windows applications that still use IE are continuously being discovered, so organizations and users need to be extra cautious and update their systems with the latest security patches.

TA-RedAnt first attacked the Korean online advertising agency server for ad programs to download ad content. They then injected vulnerability code into the server's ad content script. This vulnerability is exploited when the ad program downloads and renders the ad content. As a result, a zero-click attack occurred without any interaction from the user.

This vulnerability occurs when one type of data is mistakenly treated as another during the optimization process of IE's JavaScript engine (jscript9.dll), allowing type confusion to occur. TA-RedAnt exploited this vulnerability to trick victims into downloading malware on their desktops with the toast ad program installed. After infecting the system, various malicious behaviors can be performed, such as remote commands.

AhnLab and the NCSC immediately reported the vulnerability to Microsoft. On August 13 (local time in the U.S.), Microsoft issued CVE-2024-38178 (CVSS 7.5) and released the patch to address this vulnerability. (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38178).

Please refer to the attached report for more details.

Full Report(Korean) : (전체본)공개보고서-OperationCodeonToast.pdf
Summary Report(Korean) : (요약본)공개보고서-OperationCodeonToast.pdf

Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.

AhnLab TIP
Stay Ahead of Rapidly Evolving Threats
Make the Best-Informed Decisions
Get Started with AhnLab's State-of-the-Art Threat Intelligence
atip.ahnlab.com