# The Emergency Response Input Method High-risk Vulnerability of Antiy IEP EDR

Antiy Product Promotion Center

Time of first release: 2 August, 2024

*The original report is in Chinese, and this version is an AI-translated edition.*

## 1 Vulnerability overview

On August 1, 2024, a third-party input method was found to have a vulnerability that bypasses the login authority of windows 10 and windows 11 to execute arbitrary commands. It is concluded that this method is suitable for the mainstream Windows 10 and Windows 11 operating systems, and has been repeated on Windows 10 and Windows 11.

By using this vulnerability, the input method can bypass the system login, execute any command with the system authority, read and write files, and access the mobile media.

It should be noted that since the third-party input method has high system authority and most of the third-party input methods have many additional functions, Antiy Attack & Defense Laboratory suspects that this vulnerability will affect various third-party input methods.

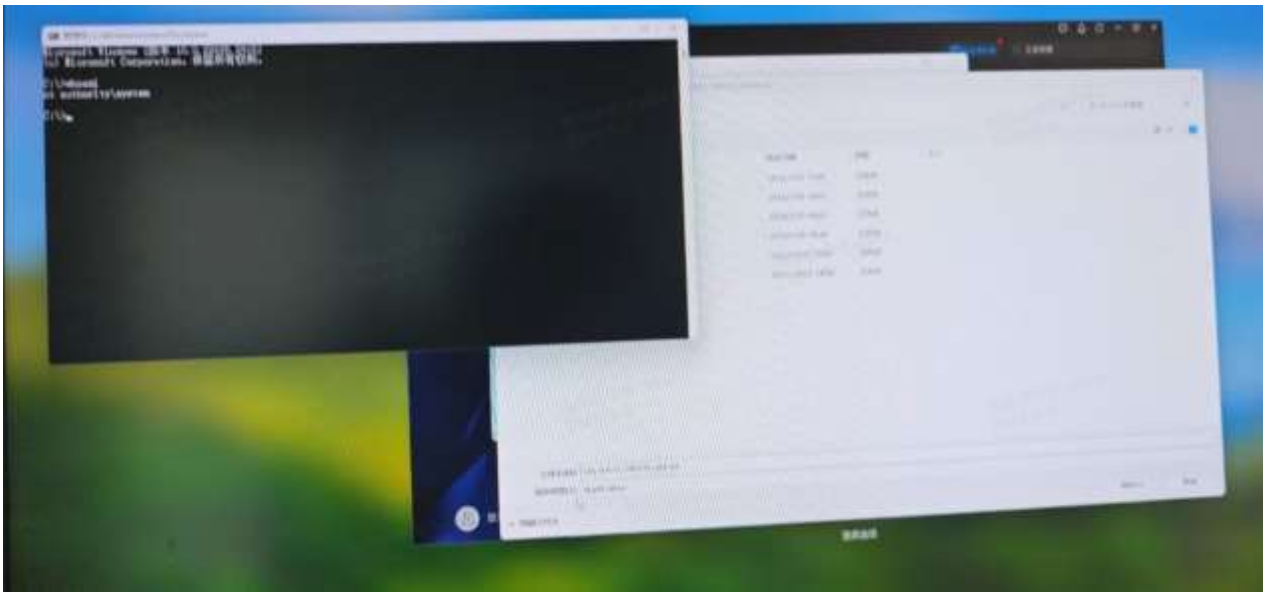

Figure 1-1 SYSTEM Permission Execution Arbitrary Instruction Verification 1

**In that scenario of local attack utilization,** the attack success rate of the vulnerability is very high.

In the remote attack utilization scenario, if the attacker logs on to the Windows host through the RDP mechanism and the Windows host turns off the network-level authentication (NLA) mechanism, the attack success rate is very high. Fortunately, NLA authentication is turned on by default in most Windows operating systems.

# 2 Vulnerability fixing

## 2.1 Official restoration status

Microsoft has not yet sent a message about the issue.

The official website of Input Method has not released the update and repair information for the moment, but the internal emergency repair should have been carried out, and it is difficult to reproduce the vulnerability in some user scenarios.

However, if there is a situation that the intranet computer cannot update the input method in time, it may still be affected by this vulnerability.

## 2.2 Manual mitigation methods

In the absence of an official fix, Antiy recommends manual mitigation for this vulnerability:

- Internal physical security shall be protected to prevent unauthorized personnel from contacting the internal computer system.
- It is unnecessary to open the RDP login authority and strictly configure the NLA mechanism.
- It is recommended to open the host of remote services, temporarily uninstall the third-party input method, and temporarily use the default input method of the system.

The way to set up the NLA mechanism is shown in Figure 2. for systems that do not require remote login, select "Do not allow remote connections to this computer." For computers that must open remote RDP login, while selecting "Allow remote connection to this computer," Be sure to check that "Only allow computer connections to run remote desktop using network level authentication" is checked below.


Figure 2-1 Set up the NLA mechanism for Windows 21

## 2.3 Defend this vulnerability by using Antiy IEP terminal detection and response system

In response to the above-mentioned vulnerabilities, the Antiy IEP terminal detection and response system added the vulnerability defense capability in the V5.0.5.1 version, and the product upgrade package has been released for the old version client. Please upgrade the IEP client to the latest version to increase the defense against the above vulnerabilities.

Antiy can start the main prevention strategy of intercepting non-microsoft system cmd to intercept the same kind of supply. However, as the strategy may affect the installation of third-party software, customers who need to adjust the strategy can contact Antiy. Our later release will open the configuration point in the EDR management and provide targeted signature rule settings.

For an upgrade package, please contact 400-840-9234.

The upgraded IEP product can effectively defend against the above vulnerabilities.


Figure 3 System alarm for terminal detection and response of intellectual armor

# 3 Security Statement

This security statement is only intended to describe any security issues that may exist and shall not be subject to any warranty or commitment by Antiy. The use of this security statement shall comply with relevant laws and regulations. Any direct or indirect consequence and loss caused by the dissemination and use of the information

provided in this security statement shall be the responsibility of the user, and the author of this security statement and the security statement shall not be liable for this.

Antiy shall have the right to revise and interpret this security statement. If you wish to reproduce or distribute this security statement, you must ensure the integrity, including the copyright notice. Without the permission of Antiy, the content of this security statement shall not be arbitrarily modified or increased, nor shall it be used for commercial purposes in any way.

## Appendix I: About Antiy IEP

Antiy IEP terminal detection and response system is a terminal security protection product for office machines, servers, special equipment and other assets. Antiy IEP has multiple protection capabilities such as asset management, risk detection, threat detection and disposal, micro-isolation and event investigation, so as to build a secure closed-loop operation system featuring endpoint identification, shaping, protection, detection and response. Implement security and effective protection of that terminal.

## Appendix II: About Antiy

Antiy is committed to enhancing the network security defense capabilities of its customers and effectively responding to security threats. Through more than 20 years of independent research and development, Antiy has developed technological leadership in areas such as threat detection engines, advanced threat countermeasures, and large-scale threat automation analysis.

Antiy has developed IEP (Intelligent Endpoint Protection System) security product family for PC, server and other system environments, as well as UWP (Unified Workload Protect) security products for cloud hosts, container and other system environments, providing system security capabilities including endpoint antivirus, endpoint protection (EPP), endpoint detection and response (EDR), and Cloud Workload Protection Platform (CWPP) , etc. Antiy has established a closed-loop product system of threat countermeasures based on its threat intelligence and threat detection capabilities, achieving perception, retardation, blocking and presentation of the advanced threats through products such as the Persistent Threat Detection System (PTD), Persistent Threat Analysis System (PTA), Attack Capture System (ACS), and TDS. For web and business security scenarios, Antiy has launched the PTF Next-generation Web Application and API Protection System (WAAP) and SCS Code Security Detection System to help customers shift their security capabilities to the left in the DevOps process. At the same time, it has developed four

major kinds of security service: network attack and defense logic deduction, in-depth threat hunting, security threat inspection, and regular security operations. Through the Threat Confrontation Operation Platform (XDR), multiple security products and services are integrated to effectively support the upgrade of comprehensive threat confrontation capabilities.

Antiy provides comprehensive security solutions for clients with high security requirements, including network and information authorities, military forces, ministries, confidential industries, and critical information infrastructure. Antiy has participated in the security work of major national political and social events since 2005 and has won honors such as the Outstanding Contribution Award and Advanced Security Group. Since 2015, Antiy's products and services have provided security support for major spaceflight missions including manned spaceflight, lunar exploration, and space station docking, as well as significant missions such as the maiden flight of large aircraft, escort of main force ships, and Antarctic scientific research. We have received several thank-you letters from relevant departments.

Antiy is a core enabler of the global fundamental security supply chain. Nearly a hundred of the world's leading security and IT enterprises have chosen Antiy as their partner of detection capability. At present, Antiy's threat detection engine provides security detection capabilities for over 1.3 million network devices and over 3 billion smart terminal devices worldwide, which has become a "national-level" engine. As of now, Antiy has filed 1,877 patents in the field of cybersecurity and obtained 936 patents. It has been awarded the title of National Intellectual Property Advantage Enterprise and the 17th (2015) China Patent Excellence Award.

Antiy is an important enterprise node in China emergency response system and has provided early warning and comprehensive emergency response in major security threats and virus outbreaks such as “Code Red”, “Dvldr”, “Heartbleed”, “Bash Shellcode” and “WannaCry”. Antiy conducts continuous monitoring and in-depth analysis against dozens of advanced cyberspce threat actors (APT groups) such as “Equation”, “White Elephant”, “Lotus” and “Greenspot” and their attack actions, assisting customers to form effective protection when the enemy situation is accurately predicted.