Antiy PTD Effectively Detects the Exploitation Behavior of the Sunflower Remote Code Execution Vulnerability

Product Department, Cybersecurity Product Center, Antiy

First draft completed: March 10, 2022

First published: March 10, 2022

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

A remote command execution vulnerability (CNVD-2022-10270) has been exposed in the Sunflower software, with a high threat level. This vulnerability affects Sunflower Personal Edition for Windows (affecting versions 11.0.0.33162 and below) and Sunflower Lite Edition (affecting version V1.0.1.43315 (December 2021)). Sunflower Remote Control is a remote control software that supports cross-platform collaboration across major operating systems including Windows, Linux, Mac, iOS, and Android. Devices with the Sunflower Remote Control client installed can be easily accessed and controlled from anywhere with an internet connection.

1 Overview

The Sunflower remote command execution vulnerability cannot be discovered on the terminal side through files. Its attack method is mainly to initiate vulnerability exploitation behavior in traffic measurement through active scanning, external remote services and other technologies, and then execute malicious code.

The Antiy PTD Network Detection Team analyzed and reproduced the CNVD-2022-10270 vulnerability in Sunflower Personal Edition (Windows). This vulnerability is caused by unauthorized access to the RPC interface of the HTTP service provided by the Sunflower client, which can obtain host information and authentication information, thereby remotely executing commands. Antiy recommends considering the following security strategies to strengthen your network:

1. Immediately upgrade the signature database of network security products, detect the network behavior characteristics of the vulnerability exploitation process, and discover attack activities that exploit the vulnerability in the network as early as possible.

2. Exposed surfaces are checked based on the traffic characteristics of Sunflower software and asset management tools.

3. In networks that process sensitive or high-value information, establish clear control policies for the use of software that uses public networks for remote assistance, and regularly review policy compliance.

2 Vulnerability Description

After analysis and verification by the Antiy PTD Network Detection Team, Sunflower Personal Edition for Windows <= 11.0.0.33162 and Sunflower Simple Edition <= V1.0.1.43315 (2021.12) have the possibility of being bypassed. The specific vulnerability information is as follows:

Table 1Vulnerability Information

Vulnerability name	Sunflower Remote Code Execution Vulnerability
Vulnerability ID	CNVD-2022-10270/CNVD-2022-03672
Affected applications and version numbers	Sunflower Personal Edition for Windows <= 11.0.0.33162 Sunflower Simple Edition <= V1.0.1.43315 (2021.12)
Vulnerability classification	Host application vulnerabilities
Vulnerability type	Unauthorized access
Vulnerability tags	Host application vulnerabilities, unauthorized access, and remote command execution
Hazard level	High
Vulnerability overview	The Sunflower remote control software has an unauthorized access vulnerability. After starting the server software, the unauthorized access port will be opened. Attackers can obtain verification information directly without a password through unauthorized access and use it to remotely execute arbitrary commands.

3 ATT&CK Mapping of Vulnerability Exploits

Analysis revealed an unauthorized access vulnerability in the Sunflower remote control software. This vulnerability allows attackers to obtain authentication information directly without a password and execute arbitrary code remotely. ATT&CK mapping revealed the technical features used by the attacker to exploit this vulnerability.

Figure 1ATT&CK mapping of vulnerability exploits

Specific ATT&CK technical behavior description table:

Table 2ATT&CK technical behavior description corresponding to the vulnerability exploitation

ATT&CK Stages/Categories	Specific Behavior	Notes
Reconnaissance	Active scan	Obtain RCE ports through scanning software, such as using xrkRCE.exe
Initial access	Leverage external remote services	Internal network resources can be accessed through the RCE port, and session credentials can be obtained
Execute	Use command and script interpreters	Construct a command execution request using session credentials
Discover	Discover remote systems	Get the system machine name and domain name
Lateral movement	Remote service session hijacking	No username or password is required, you can access it using session credentials
Collect	Automatic collection	Collect required information through remote commands
Command and Control	Use application layer protocols	Transmit control commands via HTTP

4 Detection Ideas and Vulnerability Repair Suggestions

The Antiy PTD Network Detection Team recommends that users detect Sunflower client activities. If there is an older version of the Sunflower client, it may be affected by this vulnerability. The specific detection ideas are as follows:

1. To detect activities using the Sunflower client, you can monitor the resolved domain name during Sunflower runtime and, in conjunction with the user's network behavior baseline and asset management information, discover network violations.

2. In the LAN scenario, detection is performed using vulnerability exploitation location, payload characteristics, command characteristics, server port, etc. as detection features; unauthorized acquisition of host information and lateral movement behaviors exploiting vulnerabilities are discovered within the LAN.

3. In Internet scenarios, Sunflower heartbeat and Sunflower private protocol feature activities are detected, and remote control activities in Internet scenarios are discovered based on the alarm time range.

4.1 Vulnerability Fix Suggestions

1. Temporary repair suggestions:

   1) Follow the principle of least privilege and do a good job of permission verification;

   2) Restrict access paths, implement whitelist control on user input, and implement whitelist control on executable operating system commands.

2. General repair suggestions:

The vendor has released a vulnerability fix. Users are advised to download the latest version of Sunflower (Windows 12.5.0.44969) from the official website and install it. The download address is: https://sunlogin.oray.com/download/

5 Antiy PTD Solution

The Antiy PTD network detection team analyzed and reproduced the Sunflower remote code execution vulnerability exploitation behavior based on network traffic, and promptly formulated the Sunflower vulnerability exploitation detection strategy, which has now been applied to the Antiy Persistent Threat Detection System (PTD). The Antiy PTD product can detect the use of Sunflower and vulnerability exploitation events, and can effectively detect the ATT&CK threat framework technology of multiple vulnerability exploits such as reconnaissance, initial access, execution, discovery, lateral movement, collection, command and control, etc.

Figure 2PTD's alert on the Sunflower vulnerability

Users can use Antiy PTD products to check whether there is Sunflower traffic in the network traffic, as well as the amount of Sunflower traffic, as follows:

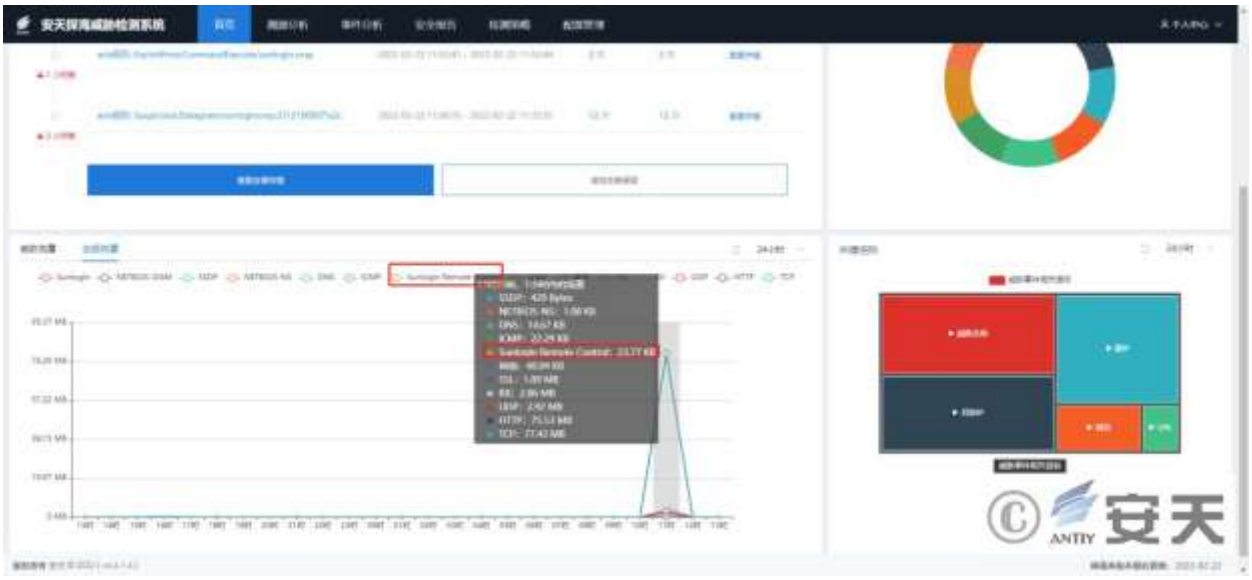

Figure 3Sunflower traffic view

Antiy PTD can detect and alert Sunflower vulnerability exploitation. For detailed event information, please view the traffic detection results in Event Analysis - > Threat Event page.

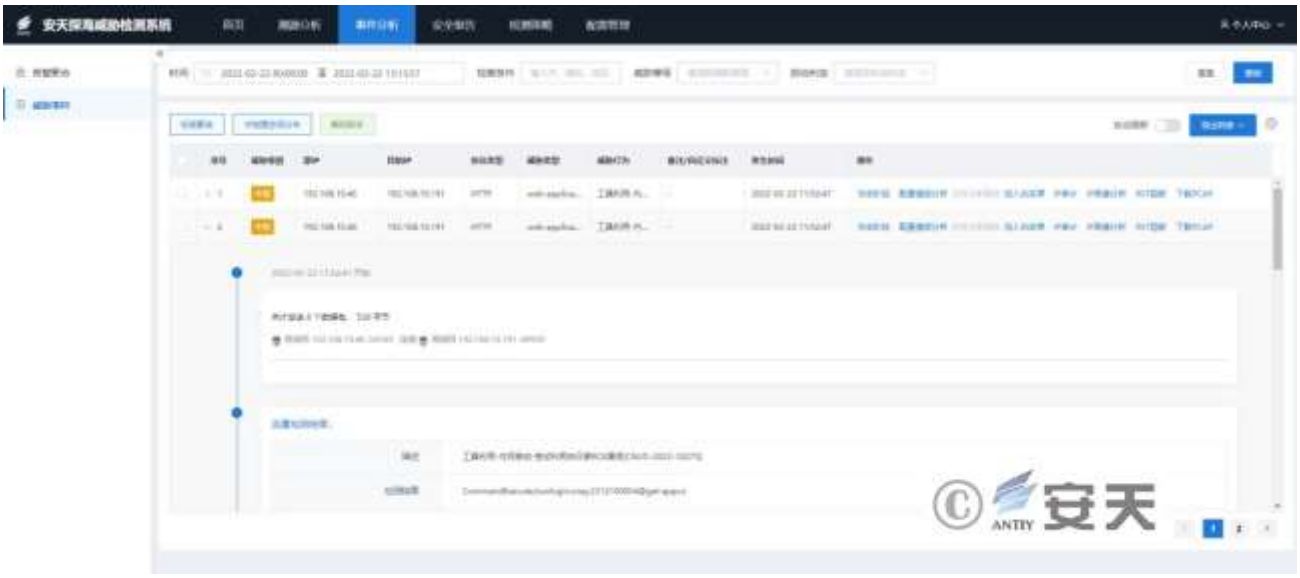

Figure 4Sunflower vulnerability exploitation incident

The PID network threat behavior rule library version that includes relevant Sunflower vulnerability exploit detection rules is: Antiy_AVLX_2022021705 (please confirm that the device system version is: 6.6.1.2 SP1 or later. It is recommended to upgrade the older version to the latest version first).

Appendix: 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.

