Nacos Remote Code Execution Vulnerability Risk Advisory

Antiy Product Promotion Center

First published: July 18, 2024

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

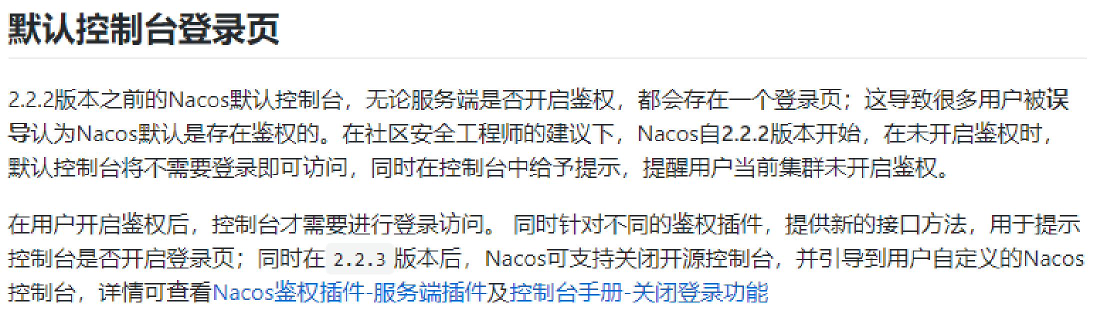
1 Vulnerability Overview

Nacos is a dynamic service discovery, configuration management and service management platform that makes it easier to build cloud-native applications. It supports a variety of out-of-the-box service-centric architecture features, seamlessly supports Kubernetes and Spring Cloud, and is an open source product with enterprise-level SLA. Recently, Antiy Attack and Defense Laboratory has monitored the relevant information of Nacos 0day and conducted follow-up analysis on this "0day" vulnerability.

2 Impact Scope

Name	Version Number
Nacos	<= v2.4.0 BETA, <= v2.3.2 As of July 16, 2024, the latest test version 2.4.0 and the latest stable version 2.3.2 are affected

According to the official documentation of Nacos, the default console of Nacos before version 2.2.2 always has a login page, regardless of whether the server has authentication enabled; this has led many users to be misled into thinking that Nacos has authentication enabled by default. Starting from version 2.2.2, when authentication is not enabled, the default console can be accessed without logging in. It has been tested that although the default configuration of version 2.2.1 before 2.2.2 has a login page, the problematic interface is still exposed, and the vulnerability can still be successfully exploited.



默认控制台登录页

2.2.2版本之前的Nacos默认控制台，无论服务端是否开启鉴权，都会存在一个登录页；这导致很多用户被误导认为Nacos默认是存在鉴权的。在社区安全工程师的建议下，Nacos自2.2.2版本开始，在未开启鉴权时，默认控制台将不需要登录即可访问，同时在控制台中给予提示，提醒用户当前集群未开启鉴权。

在用户开启鉴权后，控制台才需要进行登录访问。 同时针对不同的鉴权插件，提供新的接口方法，用于提示控制台是否开启登录页；同时在 `2.2.3` 版本后，Nacos可支持关闭开源控制台，并引导到用户自定义的Nacos控制台，详情可查看Nacos鉴权插件-服务端插件及控制台手册-关闭登录功能

3 Vulnerability Fix Methods

3.1 Official Fix Methods

Currently, the official website has not released any patches yet. Please pay attention to the official website update information in real time: https://nacos.io/download/nacos-server/

Since the vulnerability POC has been made public, it is strongly recommended that users of Nacos check the software version they are using and use the following manual mitigation methods to protect against this vulnerability.

3.2 Manual Mitigation Methods

1. Enable Authentication

According to the Nacos official document, the method to enable authentication is as follows:

1) Non-Docker Environment

Enable authentication through the application.properties configuration file.

Before enabling authentication, the configuration information in application.properties is:

```
### If turn on auth system:
nacos.core.auth.enabled=false
```

After enabling authentication, the configuration information in application.properties is:

```
### If turn on auth system:
nacos.core.auth.system.type=nacos
nacos.core.auth.enabled=true
```

2) Docker Environment

- **Official Images**

When starting the Docker container, add the following environment variables

```
NACOS_AUTH_ENABLE=true
```

For example, you can use the following command line to start the Docker environment with authentication enabled:

```
docker run --env PREFER_HOST_MODE=hostname --env MODE=standalone --env NACOS_AUTH_ENABLE=true -p 8848:8848
nacos/nacos-server
```

- **Custom Images**

To customize the image, please modify the application.properties file in the nacos project before building the image.

The following line of configuration information

```
nacos.core.auth.enabled=false
```

Modified to

```
nacos.core.auth.system.type=nacos
nacos.core.auth.enabled=true
```

Then configure the nacos startup command.

2. Set a Strong Password

Change the backend login password to a strong password. The vulnerability execution depends on the backend permissions.

3.3 Use Antiy Security Products to Enhance Detection and Defense Capabilities

1. Antiy PTF Next Generation WEB Application Protection System

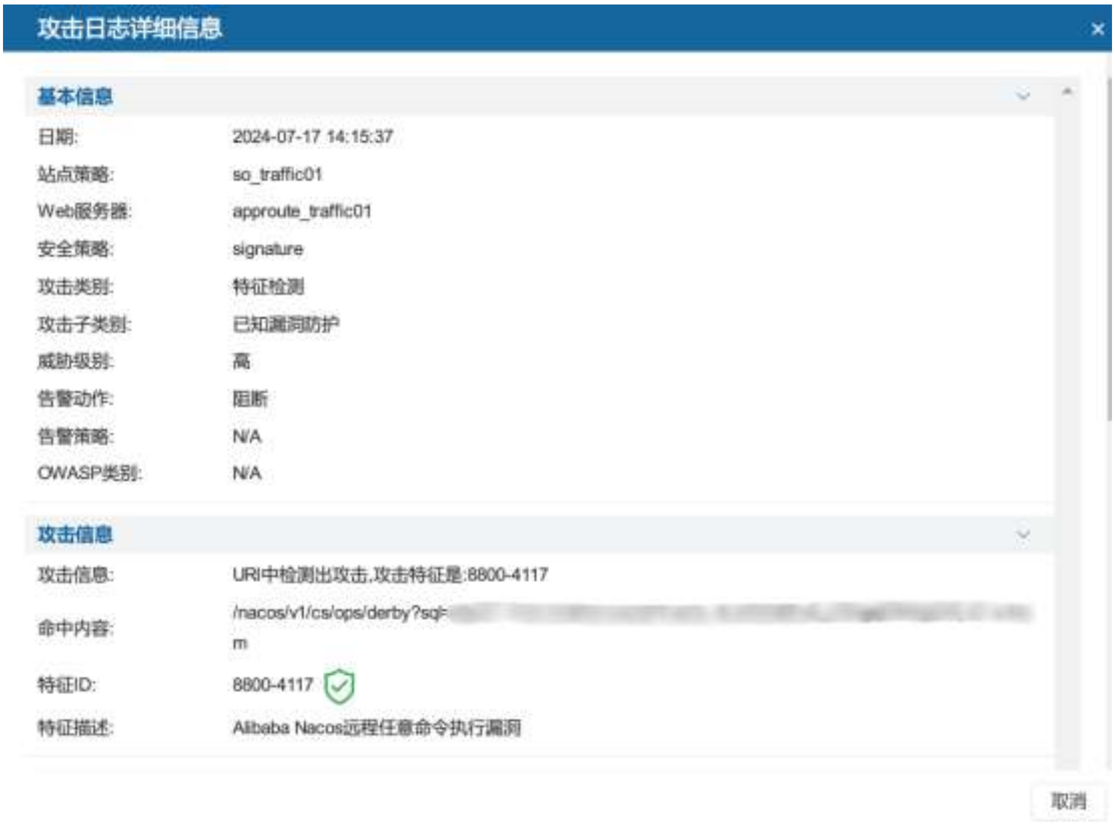
In response to the above-mentioned vulnerability, Antiy PTF next generation WEB application protection system has released a rule upgrade package, which has the ability to detect and defend against the vulnerability . Relevant users are requested to upgrade the rule package to the latest version to form security defense capabilities.

【Product upgrade package version number】

Sigdb-V2-1000-102

【Product upgrade package link】

http://iepupdate.antiy.cn/update_list/Gettoollist



攻击日志详细信息

基本信息

日期:	2024-07-17 14:15:37
站点策略:	so_traffic01
Web服务器:	approute_traffic01
安全策略:	signature
攻击类别:	特征检测
攻击子类别:	已知漏洞防护
威胁级别:	高
告警动作:	阻断
告警策略:	N/A
OWASP类别:	N/A

攻击信息

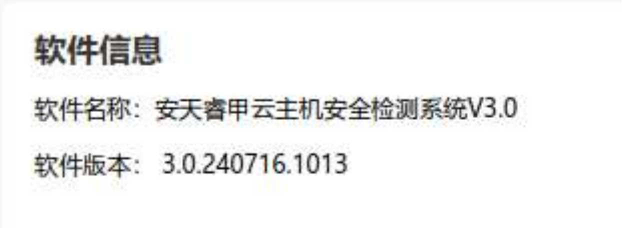
攻击信息:	URI中检测出攻击,攻击特征是:8800-4117
命中内容:	/nacos/v1/cs/ops/derby?sql=[redacted] m
特征ID:	8800-4117 ✓
特征描述:	Alibaba Nacos远程任意命令执行漏洞

2. Antiy UWP Host Security Detection Response System

In response to the above-mentioned vulnerabilities, Antiy UWP Cloud Host Security Detection System has updated its version and released the corresponding vulnerability rule feature library , which has the ability to detect the vulnerability and trace the attack source. Relevant users are requested to upgrade the rule package to the latest version to form security product detection capabilities .

【Product upgrade package link】:

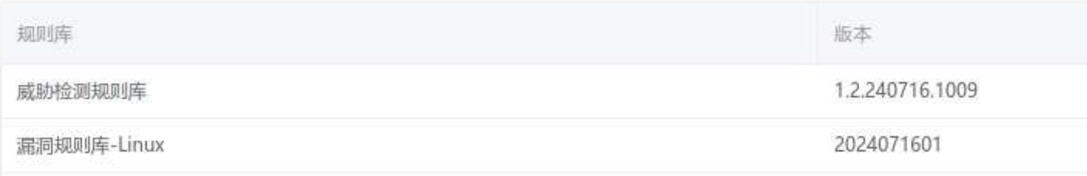
https://acs.antiy.cn/online/library/E913A64C92447C1FA87698F2142FA1E1 .zip



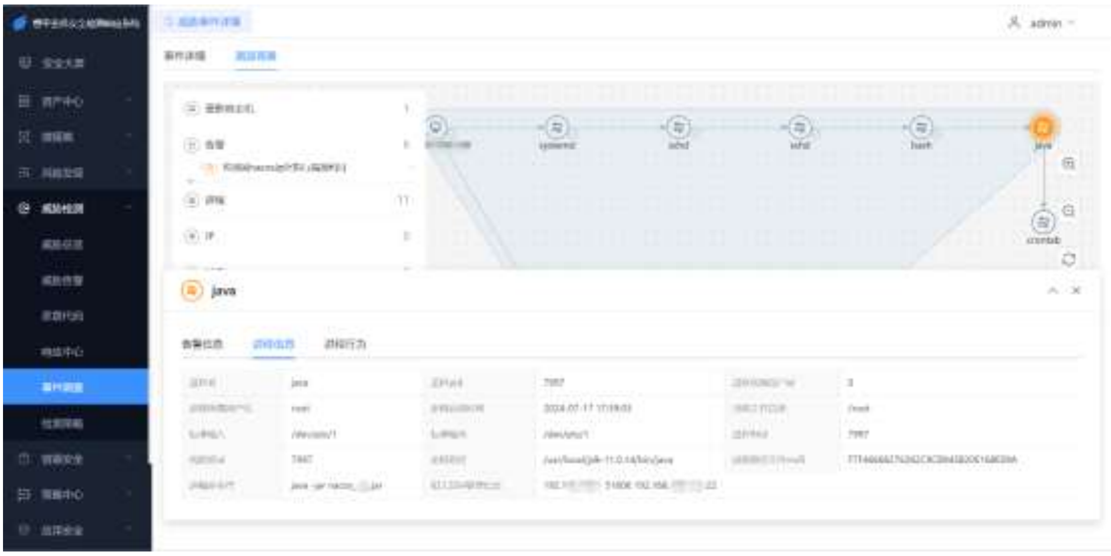
软件信息

软件名称：安天睿甲云主机安全检测系统V3.0

软件版本： 3.0.240716.1013



规则库	版本
威胁检测规则库	1.2.240716.1009
漏洞规则库-Linux	2024071601



3. Antiy Persistent Threat Detection System

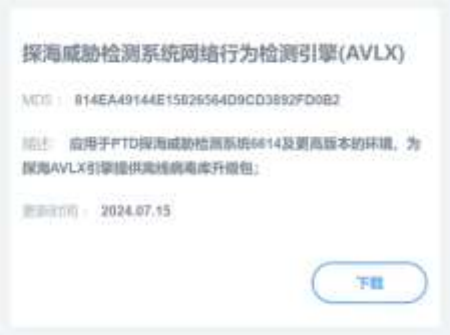
In response to the above-mentioned vulnerability, Antiy Persistent Threat Detection System has released a rule upgrade package, which has the ability to detect/defend against the vulnerability. Relevant users are requested to upgrade the rule package to the latest version to form security product detection capabilities.

【Product upgrade package version number】

Persistent Threat Detection System Network Behavior Detection Engine (AVLX)

Updated on 2024.07.15

md5 814EA49144E15826564D9CD3892FD0B2



探海威胁检测系统网络行为检测引擎(AVLX)

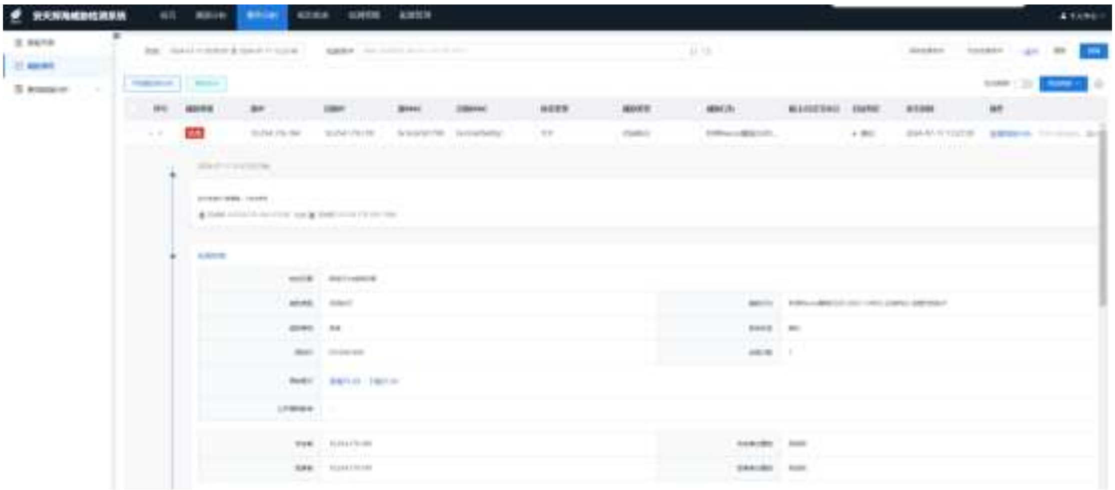
MD5： 814EA49144E15826564D9CD3892FD0B2

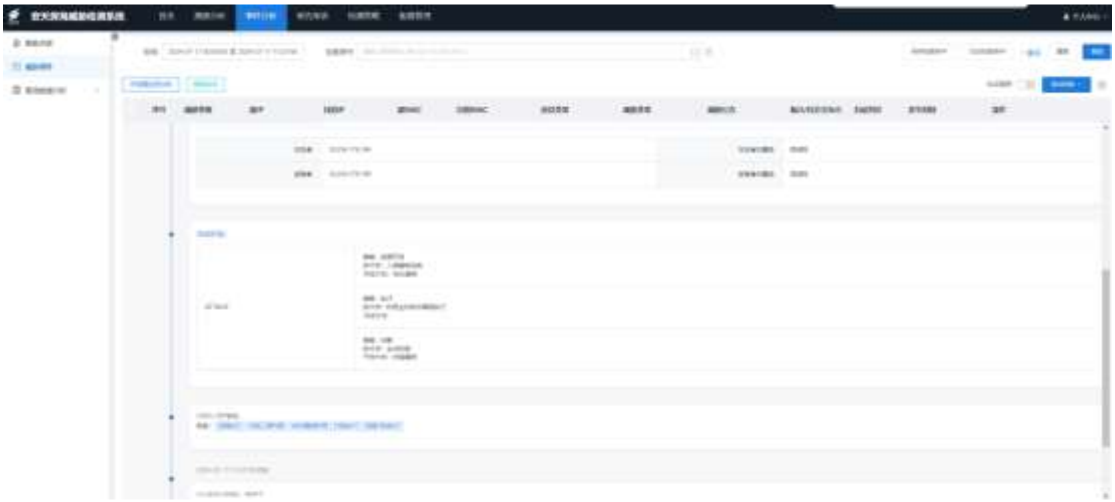
描述： 应用于PTD探海威胁检测系统6614及更高版本的环境，为探海AVLX引擎提供离线病毒库升级包；

更新时间： 2024.07.15

【Product upgrade package link】

https://iepupdate.antiy.cn/update_list/Gettoollist





4 Statement

This security bulletin is only used to describe possible security issues. Antiy does not provide any guarantee or commitment for this security bulletin. Any direct or indirect consequences and losses caused by the dissemination and use of the information provided in this security bulletin are the responsibility of the user himself, and Antiy and the author of the security bulletin do not assume any responsibility for this.

Antiy reserves the right to modify and interpret this security announcement. If you wish to reprint or disseminate this security announcement, you must ensure the integrity of this security announcement, including all contents such as the copyright statement. Without Antiy's permission, you may not arbitrarily modify or add or subtract the contents of this security announcement, and you may not use it for commercial purposes in any way.

Appendix 1: References

[1]. Nacos Documents

https://nacos.io/zh-cn/docs/v2/guide/user/auth.html

Appendix 2: About Antiy PTD Products

Antiy Persistent Threat Detection System is a capability-based network threat detection and response device independently developed by Antiy, and its core positioning is a capability-based traffic threat detection and response (NDR) product. It detects mirror traffic in real time in a bypass access mode without affecting the user's network business, helping users to discover network threats, warn of network security incidents, and support users' network security emergency response work.

Appendix 3: About Antiy UWP Products

Antiy UWP host security detection and response system integrates the concept of CWPP cloud workload protection platform. Aiming at the security protection needs of various workloads in traditional IDC and cloud business scenarios, it adopts the "one probe integrating multiple security capabilities" architecture, provides asset inventory, risk discovery, compliance baseline, micro-isolation, intrusion detection, container security, threat hunting/tracing and other security capabilities, and builds a comprehensive security monitoring, security analysis, and rapid response security protection platform.

Appendix 4: About Antiy PTF Products

Antiy PTF next generation WEB application protection system starts from the user's own business security, and provides active protection for the user's system by strengthening the security of key businesses, encapsulating dynamic data changes, and actively detecting the client environment. Through attack trapping, business obfuscation, threat intelligence integration, access tracking and other means, the system can effectively detect and defend against various attack injections, information theft, malicious page tampering, account brute force cracking, account batch registration and other attack behaviors.

Appendix V: 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.