Blog Simple.

Nagios Core 4.4.5 — URL Injection (CVE-2020-13977)

In Security Tags CVE-2020-13977, nagios, nagios core, nagios cve, nagios vulnerability June 3, 2020 1266 Views Aishee

I. OVERVIEW

- **Discoverer: Aishee – UraSec Team**
- **Vendor & Product: Nagios Core**
- **Version: Nagios Core 4.4.5**
- **CVE Reference: CVE-2020-13977**

II. ABOUT NAGIOS CORE

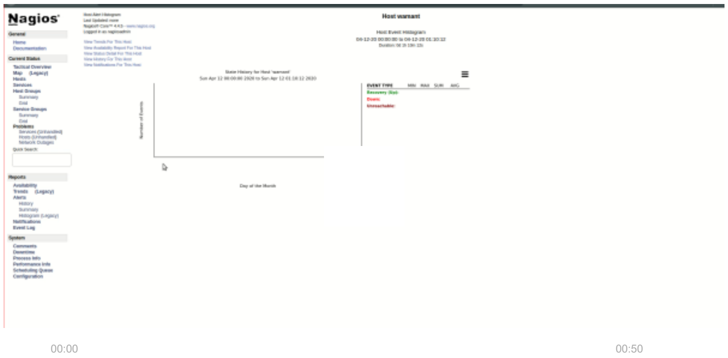
Nagios is a free and open-source computer-software application that monitors systems, networks and infrastructure. Nagios offers monitoring and alerting services for servers, switches, applications and services. It alerts users when things go wrong and alerts them a second time when the problem has been resolved.

III. VULNERABILITY DETAILS

Location: Alert Histogram and Trends function.

I could insert malicious files in Alert Histogram and Trends function, only need setup other server and compile nagios file objectjson.cgi, archivejson.cgi, statusjson.cgi and copy to server.

Video POC



IV. IMPACT

– Insert content that is harmful to users
– Ability to escalate exploits creating backdoors for applications
– ..etc

V. REMEDIATION

https://www.nagios.org/projects/nagios-core/history/4x/

https://github.com/sawolf/nagioscore/tree/url-injection-fix

VI. REPORT TIMELINE

- 04/12/2020: Discovered the vulnerability
- 04/12/2020: Responsible disclosure to Nagios Enterprise security@nagios.com
- 04/18/2020: Nagios Enterprise confirmed the issue and released a branch fix

VII. THANKS TO

- swolf@nagios.com confirm issue and fix.

Aishee

«

Previous Post:
Minimize false positives for WAF

Related Posts:

Network Security Vulnerability Assessment and Penetration Testing

Machine learning for Web Application Firewall (WAF)

Advanced Recon Automation (Subdomains) case 1

Leave a reply:

Your email address will not be published.

Name

Email

Website

Post Comment

This site uses Akismet to reduce spam. Learn how your comment data is processed.

About Me

My name is Nguyen Anh Tai. I am an independent security researcher, bug hunter and leader a security team. Security Researcher at CMC INFOSEC. I developed the every system for fun :D. My aim is to become an expert in security and xxx!

Tags

Analysis Anomaly apache attack backdoor BreakTeam bug bounty Cross Site Scripting ddos forensic hack hacking hacking waf linux linux exploit Machine Learning malware Mirai mobile analysis mobile hacking mobile pentest modsecurity nagios nagios core nagios cve nagios vulnerability nginx optimize waf OSCP OSCP for Fund OSCP Fun Guide OSCP Guide pentest pentestit php php backdoor Privilege root security SoulSec subdomain token traffic analysis waf XSS

Tweets

Aishee A good morning with Apple, x500 reward. #AppleBugBounty https://t.co/TjKDvVRKxe
about 2 months ago

Aishee SentinelOne processing and reward speed is amazing, less than 12 hours. #bugbounty https://t.co/emJYI8QHJO
about 3 months ago

Aishee @haxor31337 @ImanGurung13 Haha, When you work with them a lot, you will get used to this. Normally you will receive… https://t.co/ze28I3sdyh
about 3 months ago

Make by Aishee - A blog simple for social