NETWORK INTELLIGENCE
Global cybersecurity provider

Digest

April 2022, Edition 1.0

NETWORK INTELLIGENCE SECURITY ADVISORY

The major security news items of the month - major threats and security patch advisory. The advisory also includes IOCs and remediation steps.

IN THIS EDITION:

Security Advisory Listing		Severity
Amazon Web Services fixed Apache Log4j hot patch issues that allow container escape and privilege escalation.	🟠	High
A critical bug in Cisco Wireless LAN Controller Management Interface allows an attacker to bypass authentication controls.	🔴	Critical
Hackers are exploiting a Zero-day security flaw in the NGINX LDAP reference implementation.	🟠	High
A critical vulnerability (CVE-2021-31805) in Apache Struts leads to remote code execution.	🔴	Critical

ALSO INSIDE

Security Patch Advisory

To know more about our services reach us at info@niiconsulting.com or visit www.niiconsulting.com

Amazon Web Services fixed Apache Log4j hot patch issues that allow container escape and privilege escalation.

Severity: High

Date: April 22, 2022

BUSINESS IMPACT

Successful exploitation of the security flaws allows a malicious actor to escalate privileges, escape the container, gain root code execution, compromise neighboring services, and gain complete control over the underlying server.

RECOMMENDATIONS

1. In Kubernetes clusters, you can install the fixed hot patch version by deploying the latest Daemonset provided by AWS.

Note that only deleting the hot patch Daemonset doesn't remove the hot patch service from your nodes.

2. On standalone hosts, you can upgrade by running yum update log4j-cve-2021-44228-hotpatch.

3. Hotdog users need to upgrade to the latest version.

INTRODUCTION

In Dec 2021, Amazon released hot patches to address security flaws in environments running Java applications with a vulnerable version of the Log4j logging library or containers.

Security researchers discovered issues in AWS's Apache Log4j Hot patches that can be exploited for container escape and privilege escalation. The vulnerabilities are tracked as CVE-2021-3100, CVE-2021-3101, CVE-2022-0070, and CVE-2022-0071.

These security issues existed because the hot patch solutions invoked container binaries without properly containerizing them. Therefore, a malicious container or a malicious unprivileged process could have created and run a malicious binary named "java" to trick the hot patch solution into invoking it with elevated privileges to escape the container and take over the underlying host

AFFECTED PRODUCT

- Java-based Kubernetes applications.
- Customers using the hotpatch for Apache Log4j on Amazon Linux and Amazon Linux 2.
- Bottlerocket with the hotpatch for Apache Log4j feature enabled.

REFERENCES

- AWS's Log4Shell Hot Patch Vulnerable to Container Escape and Privilege Escalation
- Reported Apache Log4j Hotpatch Issues
- Amazon Web Services fixes container escape in Log4Shell hotfix

SECURITY ADVISORY

A critical bug in Cisco Wireless LAN Controller Management Interface allows an attacker to bypass authentication controls.

Severity: Critical

Date: April 18, 2022

BUSINESS IMPACT

Successful exploitation of the flaw could permit an unauthenticated, remote attacker to bypass the authentication process, gain administrator privileges and carry out malicious actions in a manner that allows taking complete control of an affected system.

AFFECTED PRODUCTS

This vulnerability affects the following Cisco products if they are running Cisco WLC Software Release 8.10.151.0 or Release 8.10.162.0 and have macfilter radius compatibility configured as Other:

- 3504 Wireless Controller
- 5520 Wireless Controller
- 8540 Wireless Controller
- Mobility Express
- Virtual Wireless Controller (vWLC)

RECOMMENDATIONS

1. Update Cisco Wireless LAN Controller to latest release 8.10.171.0 or later

INTRODUCTION

Cisco has released security patches to address a critical security flaw in Cisco Wireless LAN Controller (WLC). The vulnerability is tracked as CVE-2022-20695. The vulnerability exists due to the improper implementation of the password validation algorithm in the authentication functionality of Cisco Wireless LAN Controller (WLC) Software. A remote attacker can bypass authentication and log in to the device as an administrator with crafted credentials through the management interface.

CVSS Score: 10

Note: This vulnerability exists because of a non-default device configuration that must be present for it to be exploitable.

To determine whether the Cisco WLC configuration is vulnerable, issue the show mac filter summary CLI command. If RADIUS compatibility mode is other, then the device is considered to be vulnerable.

WORKAROUND

Option 1: No Macfilters in the Environment
Customers who do not use macfilters can reset the macfilter radius compatibility mode to the default value using the following CLI command:

```
wlc > config macfilter radius-compact cisco
```

Option 2: Macfilters in the Environment
Customers who use macfilters and who are able to change the radius server configuration to match other possible compatibility modes can modify the macfilter compatibility to either cisco or free using one of the following CLI commands:

```
wlc > config macfilter radius-compat cisco
wlc > config macfilter radius-compat free
```

REFERENCES

- Cisco Wireless LAN Controller Management Interface Authentication Bypass Vulnerability
- Cisco vulnerability lets hackers craft their own login credentials

Hackers are exploiting a Zero-day security flaw in the NGINX LDAP reference implementation.

Severity: High

Date: April 15, 2022

BUSINESS IMPACT

Successful exploitation of the security bug allows an attacker to potentially override the configuration parameters and bypass group membership requirements to force LDAP authentication to succeed even when the falsely authenticated user doesn't belong to the group.

AFFECTED PRODUCTS

- NGINX servers with LDAP reference implementation.

INTRODUCTION

The NGINX LDAP reference implementation uses Lightweight Directory Access Protocol (LDAP) to authenticate users of applications being proxied by NGINX. NGINX released a security advisory to address a vulnerability in the NGINX LDAP Reference Implementation. The security weakness initially surfaced on April 09th 2022, when a group called BlueHornet disclosed on Twitter an experimental exploit for NGINX 1.18.

The maintainers of the NGINX web server project have determined that only the reference implementation is affected. NGINX Open Source and NGINX Plus are not themselves affected, and no corrective action is necessary if the reference implementation is not used.

The LDAP reference implementation is impacted by the vulnerability when one of the following conditions apply:

- Command-line parameters are used to configure the Python daemon
- There are unused, optional configuration parameters
- LDAP authentication depends on specific group membership

BlueHornet hacktivist group claimed to have breached the Chinese branch of UBS Securities using the zero-day exploit.

MITIGATIONS

Mitigating Condition 1: Command-Line Parameters Are Used to Configure the Python Daemon

The primary way to configure the LDAP reference implementation is with a number of proxy_set_header directives. However, the configuration parameters can also be set on the command line that initializes the Python daemon (nginx-ldap-auth-daemon.py).

When configuration parameters are specified on the command line, an attacker can override some or all of them by passing specially crafted HTTP request headers. To protect against this, ensure that the corresponding configuration parameters have an empty value in the location = /auth-proxy block in the NGINX configuration.

Mitigating Condition 2: Unused, Optional Configuration Parameters

As in the first condition to meet the exploitation of the bug, an attacker can pass specially crafted HTTP request headers to override certain configuration parameters, depending on the configuration used for the LDAP search template. To protect against this, ensure that any unused, optional parameters have an empty value in the location = **/auth-proxy** block in the NGINX configuration.

Hackers are exploiting a Zero-day security flaw in the NGINX LDAP reference implementation.

Severity: High

Date: April 15, 2022

RECOMMENDATIONS

1. Ensure NGINX web servers are updated with latest security patches.

2. As countermeasures, NGINX recommends users to strip special characters from the username field in the login form and update appropriate configuration parameters with an empty value (“”).

3. Organizations running LDAP need to encrypt traffic using TLS certificates on IoT devices, have automated mechanisms to update IoT device firmware, and ensure the IoT device passwords are updated regularly and follow corporate policies.

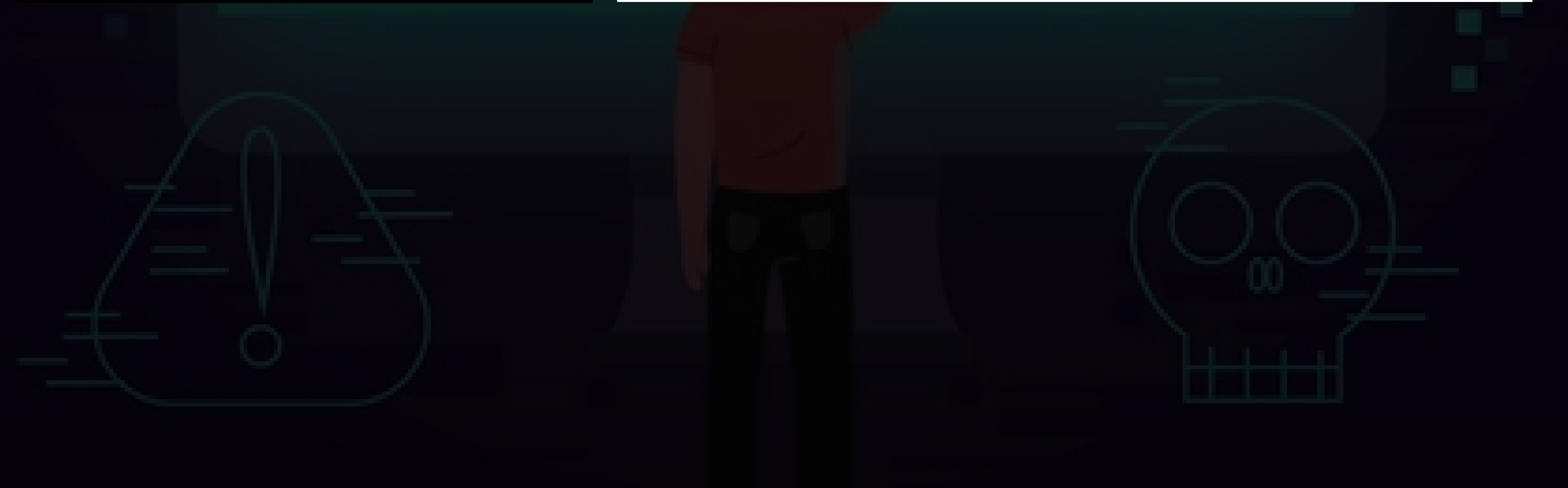
MITIGATIONS

Mitigating Condition 3: LDAP Group Membership Is Required
The Python daemon does not sanitize its inputs. Consequently, an attacker can use a specially crafted request header to bypass the group membership (memberOf) check and so force LDAP authentication to succeed even if the user is authenticated and does not belong to the required groups.

To mitigate against this, ensure that the backend daemon that presents the login form strips any special characters from the username field. In particular, it must remove the opening and closing parenthesis characters – () – and the equal sign (=), which all have special meaning for LDAP servers.

REFERENCES

- Addressing Security Weaknesses in the NGINX LDAP Reference Implementation
- NGINX zero-day vulnerability: Check if you’re affected



A critical vulnerability (CVE-2021-31805) in Apache Struts leads to remote code execution.

Severity: Critical

Date: April 14, 2022

BUSINESS IMPACT

Successful vulnerability exploitation allows a remote attacker to execute arbitrary code, take control and fully compromise a vulnerable system.

RECOMMENDATIONS

1. Upgrade Apache Struts to 2.5.30 or greater.

2. Avoid using forced OGNL evaluation on untrusted user input

INTRODUCTION

Apache has released patches to address a security flaw CVE-2021-31805 in Apache Struts2. The issue addressed by Apache fixes the previous OGNL Injection flaw CVE-2020-17530 that wasn't properly resolved. The security flaw is due to insecure OGNL usage. An attacker could exploit this vulnerability to take control of an affected system.

From Apache Struts 2.0.0 to 2.5.29, still, some of the tag's attributes could perform a double evaluation if a developer applied forced OGNL evaluation by using the %{...} syntax. Using forced OGNL evaluation on untrusted user input can lead to a Remote Code Execution and security degradation. A remote attacker can send a specially crafted request to exploit the bug and execute arbitrary code on the target system.

The security bug is more likely to be exploited in the wild by threat actors, including ransomware groups.

AFFECTED PRODUCTS

Struts 2.0.0 - Struts 2.5.29

REFERENCES

- Critical Apache Struts RCE vulnerability wasn't fully fixed, patch now
- CVE-2021-31805 RCE bug in Apache Struts was finally patched

Security Patch Advisory

11th April to 17th April | Trac- ID:NII22.04.0.3

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

UBUNTU

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
12-Apr-22	Ubuntu Linux	USN-5371-1: nginx vulnerabilities	• Ubuntu 21.10 • Ubuntu 20.04 LTS • Ubuntu 18.04 LTS • Ubuntu 16.04 ESM	Kindly update to fixed version

RED HAT

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
13-Apr-22	Red Hat Enterprise Linux	RHSA-2022:1373	• Red Hat Enterprise Linux Server - AUS 7.7 x86_64 • Red Hat Enterprise Linux Server - TUS 7.7 x86_64 • Red Hat Enterprise Linux Server (for IBM Power LE) - Update Services for SAP Solutions 7.7 ppc64le • Red Hat Enterprise Linux Server - Update Services for SAP Solutions 7.7 x86_64	Kindly update to fixed version
14-Apr-22	Red Hat JBoss Middleware	RHSA-2022:1379	• Red Hat JBoss Middleware Text Advisories for MIDDLEWARE 1 x86_64	Kindly update to fixed version

Security Patch Advisory

11th April to 17th April | Trac- ID:NII22.04.0.3

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

CISCO

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
13-Apr-22	Cisco SD-WAN	Cisco SD-WAN vManage Software Information Disclosure Vulnerability	• The vulnerability affects Cisco SD WAN vManage Software. Vulnerable Cisco SD-WAN Releases: 18.3 and earlier, 18.4, 19.2, 20.1, 20.3, 20.4, 20.5, 20.6, 20.7	Kindly update to fixed version
13-Apr-22	Cisco SD-WAN	Cisco SD-WAN vManage Software Cross Site Request Forgery Vulnerability	• The vulnerability affects Cisco SD WAN vManage Software. Vulnerable Cisco SD-WAN Releases: Earlier than 20.6, 20.6, 20.7	Kindly update to fixed version

ORACLE

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
13-Apr-22	Oracle Linux	ELSA-2022-9276 - httpd:2.4 security update	• Oracle Linux 8 (aarch64) • Oracle Linux 8 (x86_64)	Kindly update to fixed version