Log4j Zero-Day Vulnerability: What You Need to Know Now

Nick Rossmann
Global Lead
IBM Security X-Force
Threat Intelligence

Daniel Crowley
Head of Research
IBM Security X-Force Red

Abby Ross
Associate Partner
IBM Security X-Force Red

IBM **Security**

IBM

Today’s topics

- Introduction
- What is Log4j?
- What is the impact of Log4Shell?
- Who does it affect?
- How does Log4Shell work?
- What can you do to protect your organization now and in the future?

Questions about IBM products?

https://www.ibm.com/blogs/psirt/

Questions about other products?

AskXFR@ibm.com

Do you suspect you are experiencing a compromise?

X-Force’s US hotline 1-888-241-9812

Global hotline (+001) 312-212-8034

What’s Log4j?

- Log4j is a logging library embedded in thousands of the web services we use everyday.
- Developers use it to take notes about what is going on in applications and servers.
- If it was written in Java in the past decade, it’s probably in there.

How did we get here?

- December 9: Chen Zhaojun of the Alibaba Cloud Security Team discovered CVE-2021-44228, a.k.a. Log4Shell and sounded the alarm
- Security research works!

How does it work?

- Log4j takes special actions when log messages contain certain sequences that look ${like this}
- When user input such as a username in a login attempt is included in a log message, attackers can abuse Log4j features

Where is it?

- Everywhere…
  - Web facing applications
  - Middleware
  - Operational technology platforms
  - Custom solutions

Where is it?

- Everywhere…
  - Web facing applications
  - Middleware
  - Operational technology platforms
  - Custom solutions

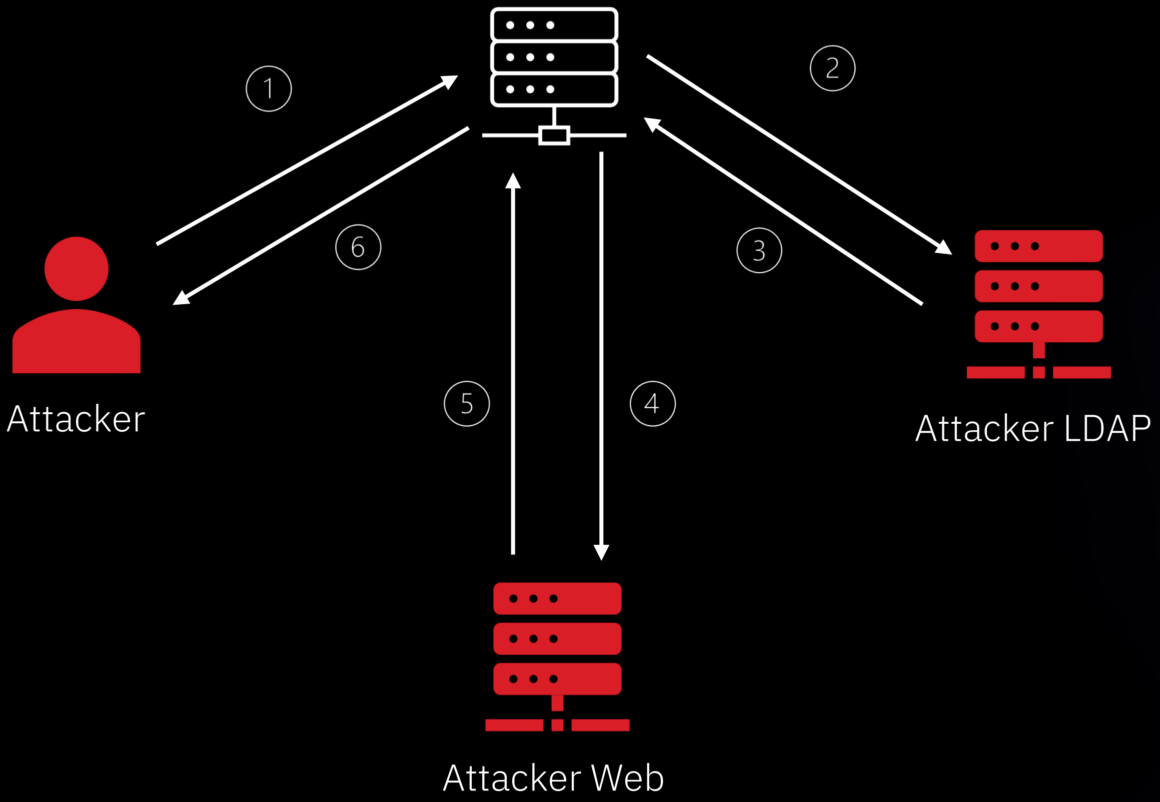
What can the adversaries do?

- Delete files
- Steal keys and other secrets
- Encrypt data for ransom
- Run a botnet
- Access internal network
- Anything Java applications are capable of!

Is anyone using it today?

- Botnets and ransomware operators are already including the exploit in their arsenal
- We will quickly see more

How does Log4Shell work?



1. Attacker sends JNDI lookup string to victim
2. Victim connects to attacker LDAP server
3. Attacker LDAP server points to Java class on attacker web server
4. Victim connects to attacker web server
5. Attacker web server responds with malicious Java class
6. Victim executes malicious Java, giving control to attacker

What can you do to protect your organization now and in the future?

1. Patch if you can

Apache released 2.16.0 to address the issue. Earlier updates 2.15.0-rc1 and 2.15.0-rc2 were found ineffective. Update if you can.

Apache also included suggested mitigations for those who cannot patch.

2. Start some scans

X-Force Red posted a custom scan tool at: https://github.com/xforcered/scan4log4shell

3. Strengthen network security controls

What servers are permitted to connect outbound to the internet?

4. Stay up to date

https://ibm.biz/log4shellioc s

Contact information

Questions about IBM products?

https://www.ibm.com/blogs/psirt/

Questions about other products?

AskXFR@ibm.com

Do you suspect you are experiencing a compromise?

X-Force's US hotline 1-888-241-9812

Global hotline (+001) 312-212-8034

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube.com/ibmsecurity

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

IBM