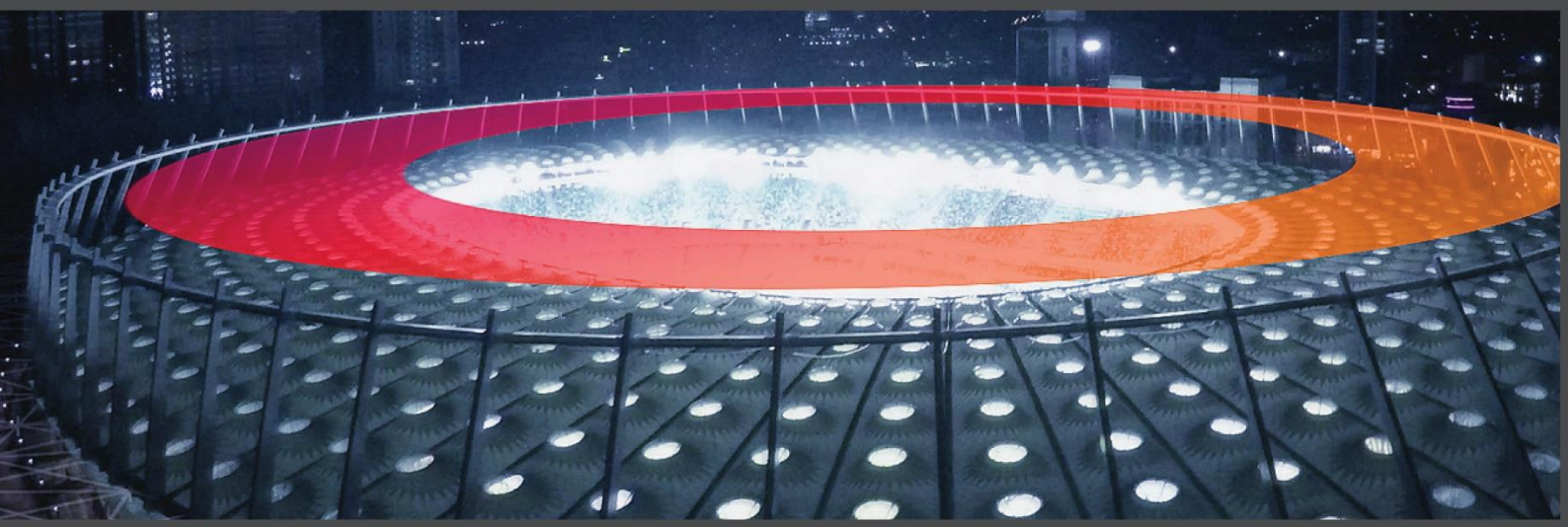
allot
See. Control. Secure.



Allot Security Advisory

Log4j2 CVE-2021-44288

See. Control. Secure.

Document Control

Position	Name	Title	Date
Author	Dudu Yosef	Product Security Group Manager	13/12/2021
Reviewer	Mark Shteiman	VP Product Management	16/12/2021
Approver	Noam Vander	Chief Information Security Officer	16/12/2021
Approver	Noam Vander	Chief Information Security Officer	23/12/2021

Revision History

Revision	Name	Changes	Date
0.1	Dudu Yosef	Initial Draft	13/12/2021
1.0	Dudu Yosef	Release	16/12/2021
2.0	Dudu Yosef	Added ClearSee reference	23/12/2021

1 CVE Details

The Apache Log4j 2 utility is a commonly used component for logging requests. On December 9, 2021, a vulnerability was reported that could allow a system running Apache Log4j 2 version 2.14.1 or below to be compromised and allow an attacker to execute arbitrary code.
On December 10, 2021, NIST published a critical Common Vulnerabilities and Exposure alert, CVE-2021-44228. More specifically, Java Naming Directory Interface (JNDI) features used in configuration, log messages, and parameters do not protect against attacker-controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from remote servers when message lookup substitution is enabled.
mitigated by setting system property "log4j2.formatMsgNoLookups" to “true” or by removing the JndiLookup class from the class path (example: zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class). Java 8u121.

From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0, this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.

1.1 Known Affected Software Versions

Logout4Shell affects Apache Log4j version 2.0.1 (including) – 2.15.0 (excluding)

1.2 Analysis Of The CVE-2021-44228 Vulnerability

The vulnerability is a remote code execution vulnerability that can allow an unauthenticated attacker to gain complete access to a target system. It can be triggered when a specially crafted string is parsed and processed by the vulnerable Log4j 2 component. This could happen through any user provided input.

Successful exploitation allows for arbitrary code execution in the targeted application. Attackers do not need prior access to the system to log the string and can remotely cause the logging event by using commands like curl against a target system to log the malicious string in the application log. When processing the log, the vulnerable system reads the string and executes it, which in current attacks is used to execute the code from the malicious domain. Doing so can grant the attacker full access and control of the affected application.

Given the fact that logging code and functionalities in applications and services are typically designed to process a variety of external input data coming from upper layers and from many possible vectors, the biggest risk factor of this vulnerability is predicting whether an

application has a viable attack vector path that will allow the malformed exploit string to reach the vulnerable Log4j 2 code and trigger the attack.

A common pattern of exploitation risk, for example, is a web application with code designed to process usernames, referrer, or user-agent strings in logs. These strings are provided as external input (e.g., a web app built with Apache Struts). An attacker can send a malformed username or set user-agent with the crafted exploit string hoping that this external input will be processed at some point by the vulnerable Log4j 2 code and trigger code execution.

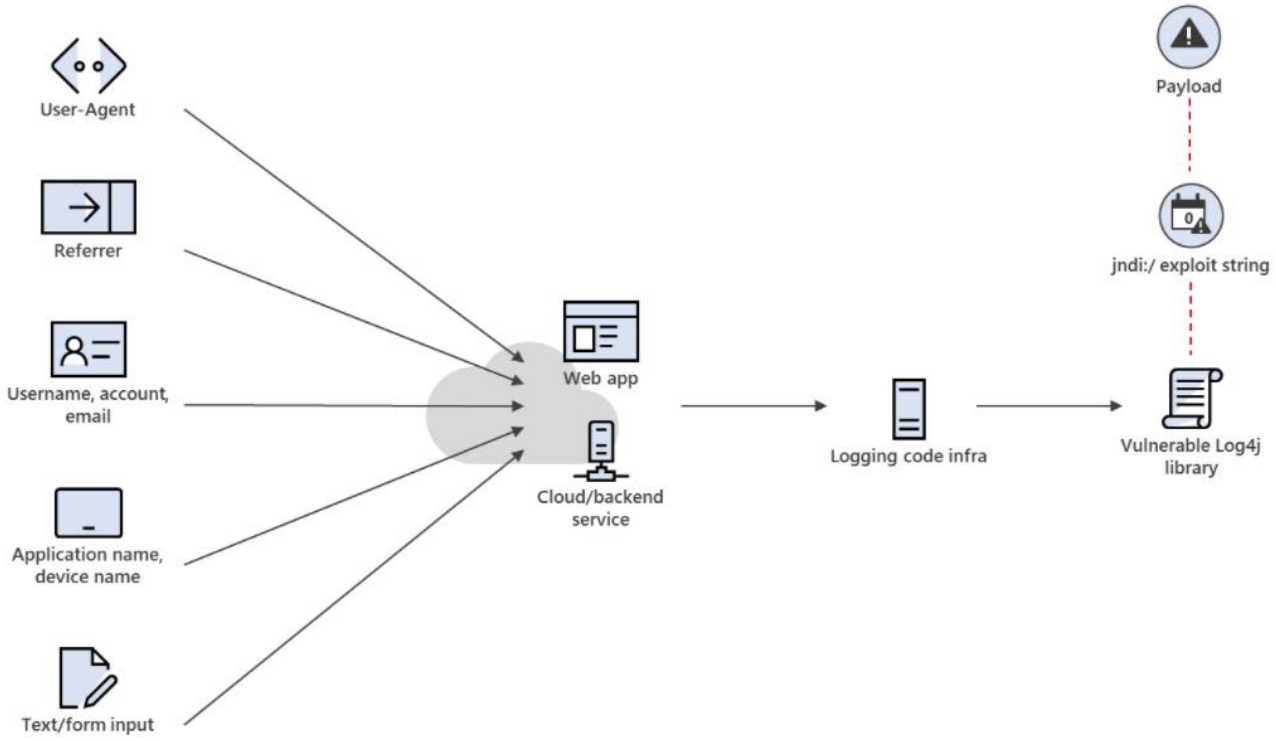


Figure 1. CVE-2021-44228 exploit vectors and attack chain

2 Affected Software Components

2.1 Allot Smart

Component	Software Version	CVE Exposure	Remediation
NetXplorer (NX)	All	None	Not applicable
Allot Operating System (AOS)	All	None	Not applicable
Data Mediator (DM)	All	None	Not applicable
DDoS Secure Controller (DSC)	All	None	Not applicable
Subscriber Management Platform (SMP)	17.1.10 / 11	Vulnerable	Hot fix will be issued by 16-DEC-2021
ClearSee	15.1.x	Vulnerable	Hot fix will be issued by 23-DEC-2021
	16.1.x		
	16.5.x		
	16.6.x - 16.9.x		
	17.1.x		
	17.2.x		

- The above table is applicable for all Allot solution deployment options, including bare metal, virtual editions (VNF) and containerized editions (CNF).

2.2 Allot Secure

Component	Software Version	CVE Exposure	Remediation
HomeSecure	All	None	Not applicable
NetworkSecure	All	None	Not applicable
Allot Secure Management	17.1	Vulnerable	Hot fix will be issued by 16-DEC-2021

3 Mitigation and Fix

Mitigation - A Security hot fix will be issued for the following versions:

- Allot Smart – SMP 17.1.10/11
- Allot Secure – ASM 17.1

4 Network Detection and Prevention of Log4j Vulnerability

In order to protect your network against Log4j vulnerability, the upcoming Allot protocol pack will give Allot Smart Enterprise customers the ability to detect and prevent the vulnerability, using a dedicated protocol signature. This adds another layer of security to your network.