Bekanntmachung: Security Bulletin 20211213-01

1. Beschreibung

Das Dienstprogramm „Apache Log4J“ in den Versionen 2.0.0 und älter, sowie 2.14.1 beinhaltet derzeit eine gravierende Schwachstelle. Diese Schwachstelle erlaubt es Angreifern per Fernsteuerung einen Schadcode auszuführen, sofern der Angreifer auf dem System einen bestimmten Zeichensatz per JNDI-LDAP-Serversuche ausführt.

2. Gefahr

Der Angreifer kann Schadsoftware durch diese Schwachstelle in das System infiltrieren und ausführen lassen.

3. IAM.cloud Stellungnahme

Eine Untersuchung der Dienste der IAM.cloud kam zu folgenden Ergebnissen:

- Die IAM.cloud Anwendungen in der Microsoft Azure Instanz verwenden keine der anfälligen Versionen des „Apache Log4J“, so dass keine weitere Maßnahmen erforderlich sind.
- Der IGAnow Gateway Service nutzt keine der vulnerablen Versionen des „Apache Log4j“ und sind dementsprechend nicht angreifbar.
- Grundsätzlich empfehlen wir unseren Kunden und Partner alle Systeme, die direkt oder indirekt mit der IAM.cloud verbunden sind und nicht originär von der IPG Group AG bereitgestellt werden, zu untersuchen, um eine versteckte Infiltration über verschiedene Wege zu vermeiden.

4. Kontakt

Für Rückfragen stehen wir gerne zur Verfügung. Entweder nutzen Sie die Ihnen benannten Kontakte oder nutzen nehmen Sie Kontakt auf unter customercare@iam.cloud.

CTO Office

IPG Information Process Group GmbH Deutschland
Hertzstraße 20
DE-13158 Berlin
Tel.: +49 30 30807135

General Manager: Marco Rohrer
Registered at the local court Berlin Charlottenburg under HRB 225816 B

www.ipg-group.com
customercare(at)iam.cloud

Announcement: Security Bulletin 20211213-01

1. Description

The "Apache Log4J" utility in versions 2.0.0 and older, as well as 2.14.1, currently contains a serious vulnerability. This vulnerability allows attackers to execute malicious code remotely if the attacker executes a certain character set on the system using a JNDI-LDAP server search.

2. Risk

The attacker can infiltrate malware into the system and execute it through this vulnerability.

3. IAM.cloud statement

An examination of the services of the IAM.cloud came to the following results:

- The IAM.cloud applications in the Microsoft Azure instance do not use any of the vulnerable versions of "Apache Log4J", so that no further actions are required.
- The IGAnow Gateway Service does not use any of the vulnerable versions of "Apache Log4j" and is therefore not vulnerable.
- In principle, we recommend our customers and partners to examine all systems that are directly or indirectly connected to the IAM.cloud and that are not originally provided by IPG Group AG in order to avoid hidden infiltration in various ways.

4. Contact

For further inquiries, we are at your disposal. Either use the contacts you have named or contact us at customer.care@ipg-group.com

CTO Office

IPG Information Process Group GmbH Deutschland
Hertzstraße 20
DE-13158 Berlin
Tel.: +49 30 30807135

General Manager: Marco Rohrer
Registered at the local court Berlin Charlottenburg under HRB 225816 B

www.ipg-group.com
customercare(at)iam.cloud