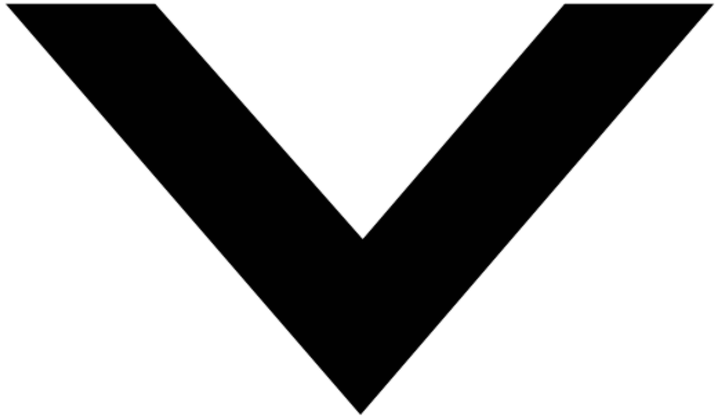

VICXER

Is Spring4Shell Really Affecting SAP ?

DISCLAIMER

- This publication contains references to the products of SAP AG. SAP, R/3, SAP NetWeaver and other SAP products and services mentioned herein are trademarks or registered trademarks of SAP AG in Germany, the US and in several other countries all over the world.

- SAP AG, the authors nor the publishers of this publication are responsible for its content. The SAP Group shall not be liable for errors or omissions with respect to the materials.

- All the information presented on this document is strictly confidential.

ABOUT US

*WE ARE **VICXER!***

- A company focused on securing the business critical applications and its adjacent infrastructure (SAP, Oracle Siebel and others)

- All of our customers belong to the Fortune-500 Group
- We do:

Oracle & SAP Penetration Testing

SAP Cyber-Security Trainings

Vulnerability Assessment and Management

SAP Forensics & Many More!

VICXER

OUR OFFICES

We are all over!

Our legal and accounting teams are in Miami, Florida, US and our execution and creative force in Buenos Aires, Argentina

VICXER

THE PROBLEM

Or what should I know about Spring4Shell ?

INTRODUCTION

VICXER

“What is the Spring Framework ?”

- It is an application framework and (IoC) for the Java platform, and it is mainly utilized to build web applications on top of the Java EE (Enterprise Edition)
- The Spring framework is open-source.
- Spring dominates the Java ecosystem, with 60% of the market-share.

INTRODUCTION

VICXER

"What is Spring4Shell ?"

- Spring4Shell is a **critical** vulnerability (CVSS v3 9.8) targeting java's most popular framework, Spring.
- It was disclosed by VMware, by the **end of March 2022**.
- The successful exploitation of this vulnerability, will allow a remote attacker to execute arbitrary execute operating system commands under the privileges of the user that is running the framework.
- A big difference between the Spring4Shell attack and his "cousin" log4shell, is that the first will actually require some pre-requisites, in order to be exploitable.
- The amount of targets that are vulnerable to Spring4Shell are **significantly smaller** than the ones that are / were vulnerable to log4shell.

IS SAP AFFECTED?

Should I be worry or this is another Scareware tactic ?

IS SAP AFFECTED ?

VICXER

"The Short answer is Yes and No"

- In April 2022, SAP has released / updated **four (4)** different SAP security notes regarding Spring4Shell.
- On the SAP security notes, SAP reflects the fact that none (at least so far) of the core technologies (SAP Netweaver / Base S4 installation) were affected by this vulnerability. This is a big relief as usually, SAP customers take extra time to patch this type of technologies, due to change control processes, regression testing, etc.
- So what specific components were affected? **SAP HANA Extended Application Services, SAP Customer Checkout, PowerDesigner Web**.
- That means all the rest of the components will **NEVER** be vulnerable ? Not really, even SAP has mentioned that other technologies my also be affected in the future.

VICXER

TAKE ACTION

A SUGGESTED ACTION PATH

How you can protect yourself and how we can help you ?

THE SOLUTION

Our Suggested Action Path …

- First of all, make sure that your team is familiar with the **SAP note 3170990**.
- If you have HANA Extended Services, Implement **SAP note 3189428.**
- If you have SAP Customer Checkout, implement **SAP note 3187290.**
- If you have PowerDesigner web, implement **SAP note 3189429.**
- Finally, consider the utilization of monitoring technologies, such as **Vicxer's Monitoring Framework**.
- **Known more on https://Vicxer.com/sap-monitoring**

THAT IS ALL…

VICXER

QUESTIONS?

To find out more about **SAP**, visit us at ***https://vicxer.com*** or follow us on Twitter

@VICXERSECURITY