Privasec | RED
RED TEAMING & ADVANCED ETHICAL HACKING

Oracle WebLogic Critical Vulnerability "Sodinokibi"

Fact Sheet v1.0 – 1st May 2019

A vulnerability dubbed "Sodinokibi" is a critical flaw within Oracle WebLogic. It is being actively exploited in the wild by remote attackers to weaponise ransomware. Oracle has released a fix and you should patch it as soon as you can, which might involve rebooting servers to apply correctly.

BACKGROUND INFORMATION

The vulnerability (CVE-2019-2725) is a deserialisation variant, resulting in remote-code execution on the affected server. There is no authentication required for attackers to exploit this flaw, other than have a connection to the host.

The result is not only a compromised server, but WebLogic servers becoming encrypted, rendering them and their attached services inoperable.

The flaw currently affects the following systems:

Oracle WebLogic Server component of Oracle Fusion Middleware

- Version 10.3.6.0.0
- Version 12.1.3.0.0

HOW IT IS EXPLOITED

An attacker sends a HTTP POST request to a server running the affected WebLogic software. Most likely, the request will contain a PowerShell command which acts as a stager – eventually downloading a malicious file (commonly, radm.exe).

Due to the flaw, the server saves the ransomware locally, then executes it – causing all files on the server to become encrypted. A ransomware page appears connecting to a TOR domain (however, there are many variants exploiting this flaw).

Another Indicator of Compromise (IoC) is that the malicious file executing 'vssadmin.exe' – a legitimate Windows utility that manages shadow copies and backups. This way, the ransomware ensures that there are no backups or copies to replace the encrypted files.

NOTE: This patch was not part of the April patch which included 53 fixes for other vulnerabilities. Administrators should explicitly patch this vulnerability.

For more information: https://www.cvedetails.com/cve/CVE-2019-2725/

CHECK THAT YOUR HOUSE IN IS ORDER

Assess your current architecture to answer the following questions:

1. Do we currently have Oracle WebLogic servers operating in our network?
2. Does the version currently match the affected versions on page 1 of this document?
3. Is the software out-of-date, unpatched or potentially susceptible to other security alerts?

Privasec can undertake high-level checks on your behalf if you are unsure of how to perform these.

I'M AFFECTED, WHAT'S THE SOLUTION?

The vendor has released a patch for this issue. Customers are advised to refer to the following link (https://www.oracle.com/technetwork/security-advisory/alert-cve-2019-2725-5466295.html) for detailed information.

Make a backup of the server, apply the patch and monitor the server closely.

BE AWARE OF THE PATCH SIDE EFFECTS

Depending on the server operating system, software programs running and usage type of your system, you may want to perform checks to ensure the patch doesn't inadvertently affect other resources, programs or network services.

While there haven't been any reports of the patch causing issues, consider making a full backup of the system before applying the patch. Store the backup off-system.

DO YOU REQUIRE ADDITIONAL ASSURANCE?

Privasec can provide you with incident response and additional assurance and peace of mind.

If you would like us to review your patching practices, perform a Penetration Test to assess potential vectors of attack or review your current network architecture, please contact us for a personalised quote.