Customer Alert 20201020

Oracle's Q4 Critical Patch Update: 20 products have bugs with CVSS scores of 9.8 or 10

Summary

The last Oracle Critical Patch Update (CPU) of 2020 includes 402 software patches across the Oracle product suite, a close follow-on to last quarter's record setting number of patches. This quarter's CPU impacts 28 product sets, 20 of which contain flaws with a CVSS rating of 9.8 or 10. A high percentage of CVEs patched in the quarterly update can be remotely exploited without user credentials including:

- 100% of Java SE CVEs
- 93% of Oracle E-Business Suite CVEs
- 78% of Fusion Middleware CVEs
- 80% of PeopleSoft CVEs

Analysis

Listen to analysis *from Waratek Founder & CTO John Matthew Holt with CEO John Adams or read select comments below.*

It's another big CPU from Oracle. Although last quarter's patch update was slightly larger, this CPU is nearly double the vulnerability count from the same time last year. There are more critical vulnerabilities in more products now than the last quarter, too Interestingly on the Java SE side this is a little bit quieter CPU. With only eight CVEs and the highest CVSS score of which is 5.3. These things fluctuate, but this quarter Java SE gets a little bit of a breather.

What jumps out to me in this CPU is I see the typical ebb and flow of vulnerability research. This is reflected in the fluctuating vulnerability counts for individual products. So now when discussing priorities and best practices for patching it's important to remind everyone that the recommendation from every software vendor including Oracle is to always apply all patches - that's for good reason. There is risk of complacency when CVSS scores in a patch for products like Java SE are lower. People might think to themselves, erroneously, there's no critical volumes this quarter, therefore, I don't need to do anything.

But here's the thing - application security doesn't work that way. Bad actors are increasingly combining vulnerabilities together to weaponize exploits to achieve their nefarious objectives. The risk score is important, but what is more important is that users and operators of these applications maintain a consistent cadence of applying these fixes as soon as they are disclosed to avoid them being weaponized in combination with other vulnerabilities to achieve a devastating result.

Next Steps

Non-Waratek customers should follow the guidelines from Oracle and that means going back to your dev test environment, pushing it through your dev test, and moving into production with all of the effort and cost and time that comes with that.

For Waratek customers, it's a very, very different, lightweight process. Take the virtual patches, take the security controls, and frankly just press the button to deploy them there and then. *You can be protected in five minutes.*

Waratek Patch and *Waratek Upgrade* customers will receive runtime virtual patches that address the Oracle CPU CVEs as part of their agreements. Virtual Patches can be deployed with no downtime to achieve instant protection. Some CVEs are also addressed in Waratek's built-in CWE rules that offer active zero-day protection with zero tuning or configuration.

Sources

Read the full Oracle October 2020 CPU news release and listen to Waratek executives discuss the last Oracle CPU of 2020.

About Waratek

Waratek is the winner of the 2020 Cyber Defense Magazine's Cutting Edge Award for Application Security, the Cybersecurity Breakthrough Award's 2019 Overall Web Security Solution of the Year, and is a previous winner of the RSA Innovation Sandbox Award along with more than a dozen other awards and recognitions. For more information, visit www.waratek.com.