waratek

Customer Alert 20211019

# October 2021 Oracle Critical Patch Update:
## *Oracle is improving security, but it comes at a price*

The October 2021 Oracle Critical Patch Update (CPU) includes 419 patches across 32 product suites, the highest number of CVEs fixed in five quarters. Of the product suites patched in the update, 26 contain vulnerabilities that can be remotely executed without user credentials. Eleven (11) product suites contain flaws with CVSS ratings of 9.1 or higher, including one (1) product with a score of 10.0. Several suites have multiple products with CVSS scores of 9.8. Also included in the patch update are the first bug fixes for the recently released Java 17.

**Comments from Waratek Founder John Matthew Holt**

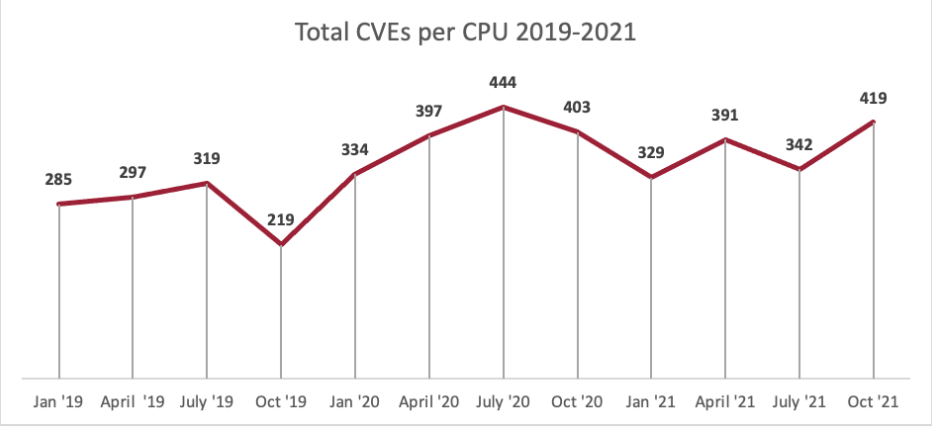
**On Java 17 Security:** *It's clear that attention is being paid to security in Java 17. There is the continued work on the hardening. Encapsulating the JDK internals and the removal of remote method invocation activation mechanism. All these things would have been unheard of years ago, but now Oracle and the community are driving these through and the reason they're doing them is for security.*

*I think the thing that people need to bear in mind, not only with Java 17 but the future versions of Java, is that as the JDK is going to be making changes to try to improve the security posture of their application, it is going to break their application. It is going to affect their application whether from a performance perspective or from a compatibility perspective.*

**On the State of Application Security:** *Patching is not working, is the way I would summarize it. It hasn't worked for a long time. It's not about to start spontaneously working now.*

*Just as we're seeing the evolution of automobiles from manual driving and as we look five years and 10 years into the future, you know, with the rise of these self-driving vehicles you can set your destination and then sit back and put your hands on your head and relax while the car takes you there. The same is happening in security, and we're seeing the same kind of rise of, if I can extend that metaphor, full self-driving security agents that attach to your app. You set the destination where you want to go. I want no insecure deserialization. I want no process forking, no SQL injection, and the agent will drive itself there and achieve that outcome for you without you having to do anything for it.*

**Listen to John Matthew's full commentary on Java 17 Security and on the State of Application Security.**



Other highlights include:

- There are 18 patches for the Oracle E-Business Suite; 4 of the CVEs can be remotely executed. The highest CVSS score is 8.1.
- There are 38 patches for Oracle Fusion Middleware; 30 of the CVEs can be remotely executed. Three (3) have a CVSS score of 9.8.
- There are 17 patches for Oracle PeopleSoft; 8 of the CVEs can be remotely executed. The highest CVSS score is 9.1.
- There are 15 Java SE patches that address CVEs, 13 of which can be remotely executed. Nine (9) of the patches fix flaws as far back as Java SE 7u311. There are 8 patches for the recently released Java 17.
- There are no indications any of the CVEs pathed in the October 2021 Critical Patch Update are currently being exploited in the wild.

**Next Steps**

Non-Waratek customers should follow the recommended guidelines from Oracle for manually propagating the updated binary patches to your development and test environments, before moving into production.

For Waratek customers, a far simpler process applies. *Waratek Patch* and *Waratek Upgrade* customers will receive ARMR virtual patches that address the Oracle CPU CVEs as part of their agreements. *Waratek Secure* customers will receive ARMR policy recommendations for enabling built-in CWE mitigations that activate zero-day protection with zero tuning or configuration.

In all cases Waratek customers achieve immediate protection to their production applications with no downtime or interruption of service. With Waratek's range of security agents, *customers are protected in five minutes or less.*

## *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.*