July 2021 Oracle Critical Patch Update:
High Severity & Remote Execution CVEs Remain the Norm

The July 2021 Oracle Critical Patch Update (CPU) includes 342 patches across 26 product suites, a slight (13 percent) decrease in CVE's patched compared to the April update. Of the product suites patched in the update, 23 contain vulnerabilities that can be remotely executed without user credentials. Sixteen (16) product suites contain flaws with CVSS ratings of 9.8 or higher, including one product with a score of 10.0. Eight (8) of the vulnerabilities can lead to insecure deserialization attacks.

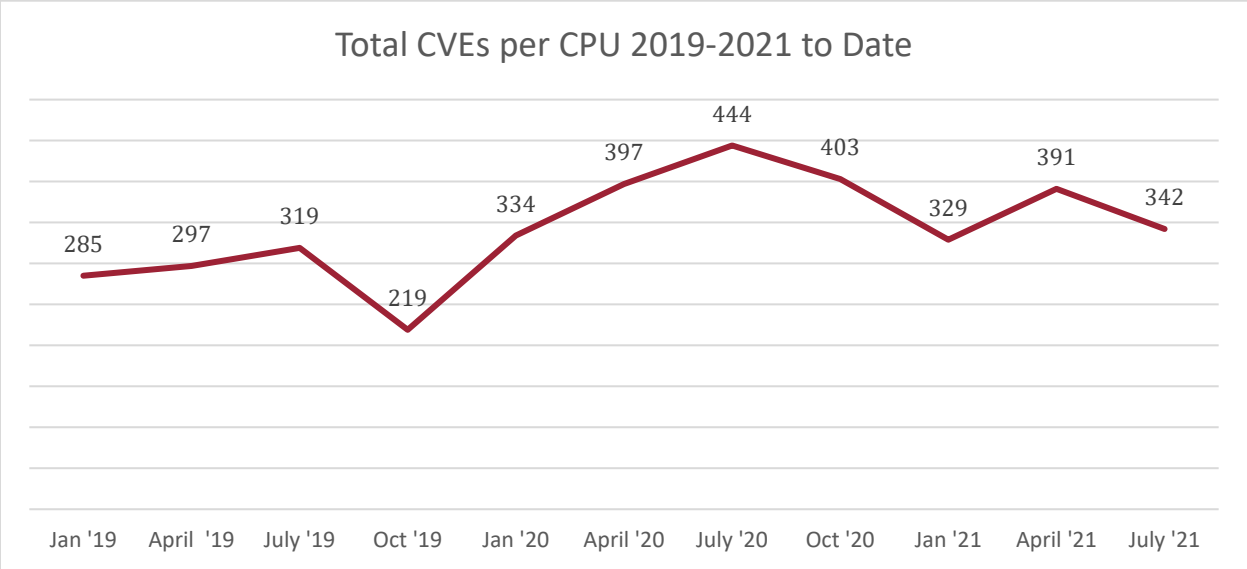
Comments from Waratek Founder John Matthew Holt

As each quarter goes, we are seeing a continuity of the same as you can see in the chart below. It's that definition of madness: Doing the same thing, expecting a different outcome. Instead here it's the same type of vulnerabilities, lots of recurring, remotely exploitable vulnerabilities. Time and again in product after product.

I think that's really the important message today. The fact that we don't see any evidence, and indeed, there is no evidence that these remote, exploitable vulnerabilities are getting less over time.

This CPU also tells us that we need new products and solutions that bring proactive security to the external third-party supply chain components that are central to some of our most important applications. Unfortunately, large bodies of application security tools like static application security testing, dynamic security testing, and DevSecOps don't add any value on the supply chain problem. The nature of supply chain is that we're bringing in code and running code that we usually don't write or we don't have control over. And so,this CPU tells me that we need new products, new solutions to address this problem.

Listen to John Matthew's full commentary here



Other highlights include:

- There are 17 patches for the Oracle E-Business Suite; 3 of the CVEs can be remotely executed. The highest CVSS score is 9.1.
- There are 48 patches for Oracle Fusion Middleware; 35 of the CVEs can be remotely executed. Two (2) have a CVSS score of 9.9 and seven (7) have a CVSS score of 9.8.
- There are 14 patches for Oracle PeopleSoft; Eight (8) of the CVEs can be remotely executed. The highest CVSS score is 9.8.
- There are six (6) Java SE patches that address CVEs, five (5) of which can be remotely executed. Three (3) of the patches fix flaws as far back as Java SE 7u301,
- There are no indications any of the CVEs pathed in the July 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.