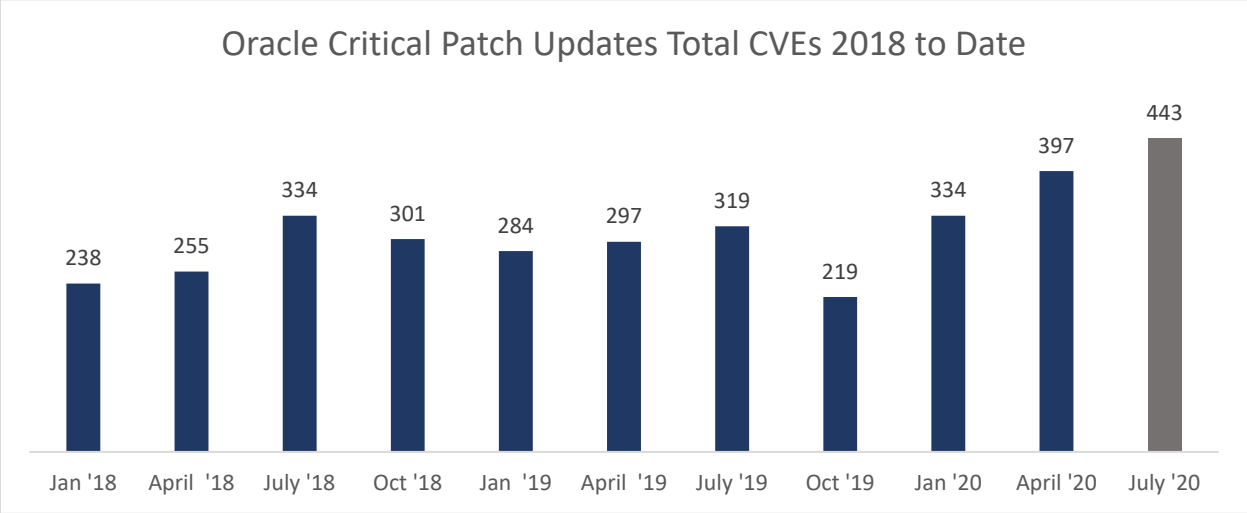
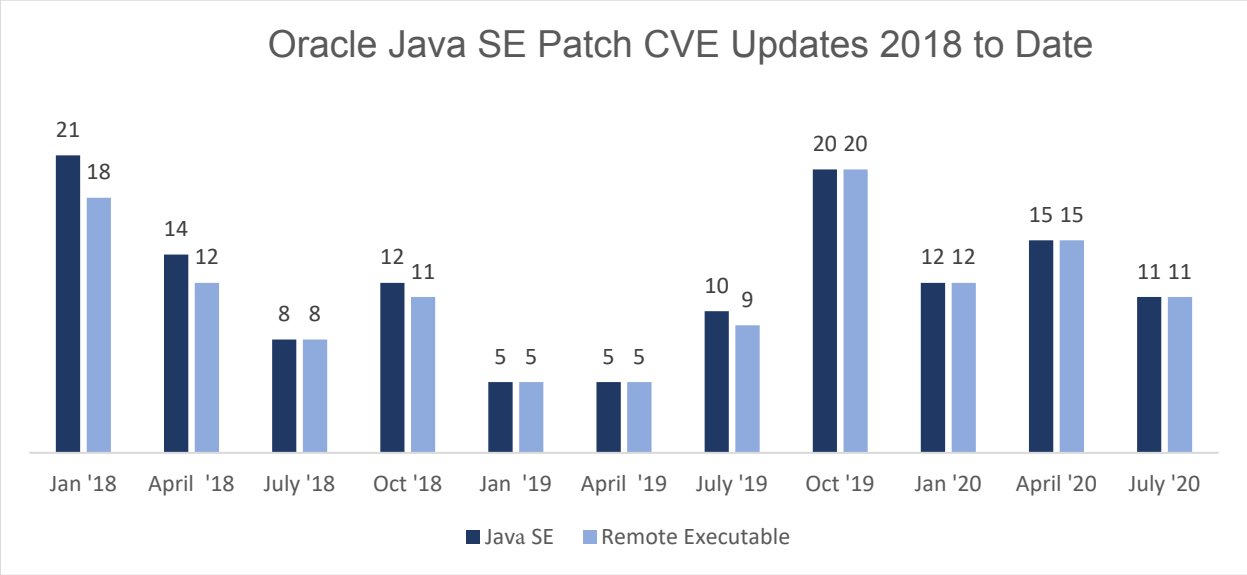
Customer Alert 20200714
Oracle's Latest Critical Patch Update is the Largest in Five Years

The July Oracle 2020 Critical Patch Update (CPU) fixes a record 443 CVEs across the Oracle product suite according to the company's quarterly announcement. The CPU patches flaws across 29 products, many of which carry a "critical" severity rating and a high percentage of which can be remotely exploited without user credentials. The CPU includes:

- 11 patches for Java SE, 11 of which can be remotely executed
- 52 patches for Oracle Fusion Middleware, 48 of which can be remotely executed
- 30 patches for Oracle E-Business Suite, 24 of which can be remotely executed
- 11 patches for Oracle PeopleSoft, 9 of which can be remotely executed





Waratek's Advice to Customers & Prospects

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.

Non-customers should follow Oracle's advice and apply the critical patch updates without delay.

Q3 CPU Java SE highlights

- Java SE is still the most widely used programming language for enterprise applications, and 100 percent of the vulnerabilities patched in the July CPU can be remotely exploited, including flaws in versions as old as Java 7 and as recent Java 14. This continues a years-long trend of the majority of Java flaws being open to remote execution.
- There are a total of 11 new fixes in Java SE, with the highest CVSS score being 8.3.
- The CPU for Java SE release patches flaws in Java SE versions 7u261, 8u251, 11.0.7, and 14.0.1
- JDK 8u261 includes an implementation of the Transport Layer Security (TLS) 1.3 specification (RFC 8446). TLS 1.3 is disabled for default SSLContext("SSL" or "TLS") for client end-point. Note that TLS 1.3 is not directly compatible with previous versions.
- There are no Critical vulnerabilities fixed in Java SE. 27% of the fixed vulnerabilities are high severity; another 27% are medium and the rest are low severity.
- 36% of the fixed vulnerabilities are fixes in the core libraries of Java SE.

Regarding other Oracle products

- Fifteen (15) Oracle products include patches for CVEs with a CVSS 3.0 base score of 9.0 or higher, including one product – Oracle Communications Applications - with 10.0 score. Ten products have at least one CVE rated 9.8.
- Fusion Middleware fixed 52 CVEs, 48 of which may be remotely exploited without authentication. Highest CVSS v3.1 base score is 9.8.
- About 20% of the fixes in the WebLogic server are fixes for deserialization vulnerabilities that could allow the complete compromise of the system.
- CVE-2020-14622 was patched that allows arbitrary file read vulnerability in the WebLogic server.

Read the full Oracle CPU news release here.

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.