PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Primavera-Products-Suite] Oracle Primavera P6 Enterprise Project Portfolio Management Remote Unspecified Vulnerability in Web Access	Oracle Primavera P6 Enterprise Project Portfolio Management versions 8.2, 8.3, 8.4, 15.1, 15.2, 16.1, and 16.2 is prone to a remote unspecified vulnerability in Web Access. An unauthenticated remote attacker could exploit this issue to affect confidentiality, integrity, and availability.	Version(s): Oracle Primavera P6 Enterprise Project Portfolio Management versions 8.2, 8.3, 8.4, 15.1, 15.2, 16.1, and 16.2	Published - January 17, 2017 CVE-2017-3324 CVSS - 9.4 Vendor's Advisory Available at : https://www.oracle.com/technetwork/topics/security/cpujan2017-2881727.html
Oracle Java SE, Java SE Embedded and JRockit Remote Code Execution in RMI	Oracle Java SE 6 SE through 6 SE update 131, 7 SE through 7 SE update 121, 8 SE through 8 SE update 112, 8 Embedded through 8 Embedded update 111 and JRockit R28.3.12 allow a remote attacker to execute arbitrary code via vectors related to RMI. This vulnerability can only be exploited by supplying data to APIs in the specified component without using Untrusted Java Web Start applications or Untrusted Java applets.	Version(s): Oracle Java SE 6 SE through 6 SE update 131, 7 SE through 7 SE update 121, 8 SE through 8 SE update 112, 8 Embedded through 8 Embedded update 111 and JRockit R28.3.12	Published - January 17, 2017 CVE-2017-3241 CVSS - 10.0 Vendor's Advisory Available at: https://www.oracle.com/technetwork/topics/security/cpujan2017-2881727.html
Oracle Java SE and Java SE Embedded Remote Code Execution in Libraries	Oracle Java SE 6 SE through 6 SE update 131, 7 SE through 7 SE update 121, 8 SE through 8 SE update 112 and 8 Embedded through 8 Embedded update 111 allow a remote attacker to execute arbitrary code via vectors related to Libraries. This issue applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code and rely on the Java sandbox for security. This issue does not apply to Java deployments, typically in servers, that load and run only trusted code.	Version(s): Oracle Java SE 6 SE through 6 SE update 131, 7 SE through 7 SE update 121, 8 SE through 8 SE update 112 and 8 Embedded through 8 Embedded update 111	Published - January 17, 2017 CVE-2017-3272 CVSS - 9.3 Vendor's Advisory Available at: https://www.oracle.com/technetwork/topics/security/cpujan2017-2881727.html
Oracle One-to-One Fulfillment Remote Unspecified Vulnerability in Internal Operations	Oracle One-to-One Fulfillment versions 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, and 12.2.6 is prone to a remote unspecified vulnerability in Internal Operations. An unauthenticated remote attacker could exploit this issue to affect confidentiality and integrity.	Version(s):Oracle One-to-One Fulfillment versions 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, and 12.2.6	Published - January 17, 2017 CVE-2016-8325 CVSS - 9.4 The vendor's advisory is available at: http://www.oracle.com/technetwork/security-advisory/cpujan2017-2881727.html
Adobe Flash Player <=24.0.0.186 Remote Memory-Corruption Vulnerability	Adobe Flash Player versions 24.0.0.186 and earlier have an exploitable memory corruption vulnerability related to the parsing of SWF metadata. Successful exploitation could lead to arbitrary code execution.	Version(s): Adobe Flash Player versions 24.0.0.186 and earlier	Published -January 10,2017 CVE-2017-2931 CVSS - 9.3 Vendor's Advisory Available at https://helpx.adobe.com/security/products/flash-player/apsb17-02.html
Adobe Flash Player <=24.0.0.186 Remote Use-After-Free Vulnerability	Adobe Flash Player versions 24.0.0.186 and earlier have an exploitable use after free vulnerability in the ActionScript FileReference class, when using class inheritance. Successful exploitation could lead to arbitrary code execution.	Version(s): Adobe Flash Player versions 24.0.0.186 and earlier	Published -January 10, 2017 CVE-2017-2937 CVSS - 9.3 The vendor's advisory is available at: https://helpx.adobe.com/security/products/flash-player/apsb17-02.html
Apple iOS <10.2.1 Remote Code Execution Vulnerability in WebKit	Apple iOS before 10.2.1 is prone to a remote code execution vulnerability in WebKit due to a memory corruption issue. A remote attacker could exploit this issue to execute arbitrary code on the affected system by enticing the user to visit a maliciously crafted webpage.	Version(s): Apple iOS before 10.2.1	Published -January 23,2017 CVE-2017-2356 CVSS - 9.3 Vendor's Advisory Available at https://support.apple.com/en-il/HT207482l
Apple MacOS X <10.12.3 Remote Code Execution Vulnerability in Kernel	Apple MacOS X before 10.12.3 is prone to a remote code execution vulnerability in Kernel. A remote attacker could exploit this issue to execute arbitrary code with kernel privileges on the affected system via a crafted application.	Version(s): Apple MacOS X before 10.12.3	Published -January 23, 2017 CVE-2017-2370 CVSS - 9.3 The vendor's advisory is available at: https://support.apple.com/en-il/HT207483
Apple WatchOS <3.1.3 Remote Privilege Escalation Vulnerability in the Kernel	Apple WatchOS before 3.1.3 is prone to a remote privilege escalation vulnerability in the Kernel due to a memory corruption issue. A remote attacker could exploit this issue, via a crafted application, to execute arbitrary code with kernel privileges on the affected system.	Version(s): Apple WatchOS before 3.1.3	Published -January 23,2017 CVE-2016-7606 CVSS - 9.3 Vendor's Advisory Available at https://support.apple.com/en-il/HT207487
Apple MacOS X <10.12.3 Remote Code Execution Vulnerability in Graphics Drivers	Apple MacOS X before 10.12.3 is prone to a remote code execution vulnerability in Graphics Drivers due to a memory corruption issue. A remote attacker could exploit this issue to execute arbitrary code with kernel privileges on the affected system via a crafted application.	Version(s):Apple MacOS X before 10.12.3	Published -January 23, 2017 CVE-2017-2358 CVSS - 9.3 The vendor's advisory is available at: https://support.apple.com/en-il/HT207483