National Cyber Awareness System

SB17-100: Vulnerability Summary for the Week of April 3, 2017

04/10/2017 07:48 AM EDT

Original release date: April 10, 2017

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center(NCCIC) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Risk Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves mishandling of profile uninstall actions in the "MCX Client" component when a profile has multiple payloads. It allows remote attackers to bypass intended access restrictions by leveraging Active Directory certificate trust that should not have remained.	2017-04-01	7.5	CVE-2017-2402 BID CONFIRM

apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "IOATAFamily" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-04-01	9.3	CVE-2017-2408 BID CONFIRM
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context via a crafted app.	2017-04-01	9.3	CVE-2017-2410 BID CONFIRM
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "Bluetooth" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-04-01	9.3	CVE-2017-2420 BID CONFIRM
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "AppleGraphicsPowerManagement" component. A race condition allows attackers to execute arbitrary code in a privileged context via a crafted app.	2017-04-01	9.3	CVE-2017-2421 BID CONFIRM
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "Multi-Touch" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-04-01	9.3	CVE-2017-2422 BID CONFIRM

apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "Bluetooth" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-04-01	9.3	CVE-2017-2427 BID CONFIRM
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "IOFireWireAVC" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-04-01	9.3	CVE-2017-2436 BID CONFIRM
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "IOFireWireAVC" component. It allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors.	2017-04-01	7.2	CVE-2017-2437 BID CONFIRM
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "AppleRAID" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (use-after-free) via a crafted app.	2017-04-01	9.3	CVE-2017-2438 BID CONFIRM
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "Intel Graphics Driver" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-04-01	9.3	CVE-2017-2443 BID CONFIRM

apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "Bluetooth" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (use-after-free) via a crafted app.	2017-04-01	9.3	CVE-2017-2449 BID CONFIRM
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "libxslt" component. It allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.	2017-04-01	7.5	CVE-2017-2477 BID CONFIRM