Security Advisory | Volume 2017-073-1

PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Microsoft Security Update for Adobe Flash Player Use-After-Free Issue	Adobe Flash Player versions 24.0.0.194 and earlier, running on Windows 8.1, Windows Server 2012, Server 2012 R2, Windows 10 and Windows Server 2016, have an exploitable use after free vulnerability in a routine related to player shutdown. Successful exploitation could lead to arbitrary code execution.	Version(s): Adobe Flash Player versions 24.0.0.194 and earlier, running on Windows 8.1, Windows Server 2012, Server 2012 R2, Windows 10 and Windows Server 2016	Published - February 21, 2017 CVE-CVE-2017-2982 CVSS - 9.3 Vendor's Advisory Available at :https://helpx.adobe.com/security/products/flash-player/apsb17-04.html
Mozilla Firefox <52 Remote Code Execution due to Several Memory Safety Issues	Mozilla Firefox before 52 allows remote attackers to execute arbitrary code due to several memory safety issues.	Version(s): Mozilla Firefox before 52	Published - March 07, 2017 CVE-2017-5399 CVSS - 9.3 Vendor's Advisory Available at: https://www.mozilla.org/en-US/security/advisories/mfsa2017-05/
Mozilla Firefox <52 Remote Code Execution due to Use-After-Free in AddRange	Mozilla Firefox before 52 is prone to a remote use-after-free vulnerability. A remote attacker could exploit this issue by using addRange to add range to an incorrect root object. Successful exploitation would result in a denial-of-service condition, and possibly allow arbitrary code execution.	Version(s): Mozilla Firefox before 52	Published - March 07, 2017 CVE-2017-5403 CVSS - 9.3 Vendor's Advisory Available at : https://www.mozilla.org/en-US/security/advisories/mfsa2017-05/
Mozilla Firefox, Firefox ESR and Thunderbird Remote Memory Corruption Vulnerabilities	Mozilla Firefox before 52, Firefox ESR before 45.8 and Thunderbird before 45.8 are prone to multiple memory safety bugs, some of which may allow remote code execution via memory corruption.	Version(s): Mozilla Firefox before 52, Firefox ESR before 45.8 and Thunderbird before 45.8	Published - March 07, 2017 CVE-2017-5398 CVSS - 9.3 Vendor's Advisory Available at: https://www.mozilla.org/en-US/security/advisories/mfsa2017-07/
Mozilla Firefox, Firefox ESR and Thunderbird Remote Code Execution Related to FontFace Objects	Use-after-free in Mozilla Firefox before 52, Firefox ESR before 45.8 and Thunderbird before 45.8 allows a remote attacker to execute arbitrary code while handling events related to FontFace objects.	Version(s): Mozilla Firefox before 52, Firefox ESR before 45.8 and Thunderbird before 45.8 .	Published - March 07, 2017 CVE-2017-5402 CVSS - 9.3 Vendor's Advisory Available at : https://www.mozilla.org/en-US/security/advisories/mfsa2017-07/
Google Android <=7.1.1 Remote Escalation of Privileges in Qualcomm Camera Driver	Qualcomm Camera Driver in Google Android 7.1.1 and earlier before 2017-03-05 on Nexus 5X, Nexus 6, Nexus 6P, Android One, Pixel and Pixel XL allows a remote attacker to cause a denial-of-service via a local malicious application , aka Android internal bug 32342399.	Version(s): Google Android 7.1.1 and earlier before 2017-03-05 on Nexus 5X, Nexus 6, Nexus 6P, Android One, Pixel and Pixel XL	Published - March 06, 2017 CVE-2016-8417 CVSS - 9.3 Vendor's Advisory Available at: https://source.android.com/security/bulletin/2017-03-01.html
Google Android <=7.1.1 Remote Code Execution in Qualcomm Bootloader	Qualcomm bootloader in Google Android 7.1.1 and earlier before 2017-03-05 on Pixel and Pixel XL allows a remote attacker to execute arbitrary code via a crafted application, aka Android internal bug 32370952.	Version(s): Google Android 7.1.1 and earlier before 2017-03-05 on Pixel and Pixel XL .	Published - March 06, 2017 CVE-2017-0455 CVSS - 9.3 Vendor's Advisory Available at : https://source.android.com/security/bulletin/2017-03-01.html
Google Android 7.1.1 and Earlier Remote Privilege Escalation in MediaTek APK	MediaTek APK in Google Android 7.1.1 and earlier, before 2017-03-05 could allow remote attackers to execute arbitrary code with high privileges via a crafted application. Aka Android internal bug 32916158.	Version(s):Google Android 7.1.1 and earlier, before 2017-03-05.	Published - March 06, 2017 CVE-2017-0522 CVSS - 9.3 Vendor's Advisory Available at: http://source.android.com/security/bulletin/2017-03-01.html
Google Android <=7.1.1 Remote Escalation of Privileges in Qualcomm Networking Driver	Qualcomm Networking driver in Google Android 7.1.1 and earlier before 2017-03-05 allows a remote attacker to execute arbitrary code via a crafted application.	Version(s): Google Android 7.1.1 and earlier before 2017-03-05	Published - March 07, 2017 CVE-2017-0460 CVSS - 9.3 Vendor's Advisory Available at : https://source.android.com/security/bulletin/2017-03-01.html
Google Android <=7.1.1 Remote Code Execution in Libgdx	Libgdx in Google Android 7.1.1 and earlier before 2017-03-01 allows a remote attacker to execute arbitrary code via a crafted file.	Version(s): Google Android 7.1.1 and earlier before 2017-03-01.	Published - March 06, 2017 CVE-2017-0477 CVSS - 9.3 Vendor's Advisory Available at: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0477
Google Android <=7.1.1 Privilege Escalation in Kernel Networking Subsystem via a Crafted Application	Google Android 7.1.1 and earlier before 2017-03-05, when running on Nexus 5X, Nexus 6P, Pixel, and Pixel XL, is prone to a privilege escalation vulnerability in the kernel networking subsystem. A remote attacker could exploit this issue via a crafted application to execute arbitrary code on the system with kernel privileges. AKA Android internal bug 33753815.	Version(s): Google Android 7.1.1 and earlier before 2017-03-05, when running on Nexus 5X, Nexus 6P, Pixel, and Pixel XL.	Published - March 06, 2017 CVE-2016-10200 CVSS - 9.3 Vendor's Advisory Available at : http://source.android.com/security/bulletin/2017-03-01.html
Google Android <=7.1.1 Remote Privilege Escalation in NVIDIA GPU Driver	NVIDIA GPU driver in Google Android 7.1.1 and earlier on Pixel C before 2017-03-05, could allow remote attackers to execute arbitrary code with kernel privileges via a crafted application, aka Android internal bug 33899363.	Version(s): Google Android 7.1.1 and earlier on Pixel C before 2017-03-05.	Published - March 05, 2017 CVE-2017-0333 CVSS - 9.3 Vendor's Advisory Available at: https://source.android.com/security/bulletin/2017-03-01.html
Google Android Privilege Escalation in Kernel Networking Subsystem via a Crafted Application	Race condition in the netlink_dump function in net/netlink/af_netlink.c in the Linux kernel, as used in Google Android 7.1.1 and earlier before 2017-03-05 on Pixel C, Pixel, and Pixel XL, allows remote attackers to cause a denial of service (double free) or possibly have unspecified other impact via a crafted application that makes sendmsg system calls, leading to a free operation associated with a new dump that started earlier than anticipated. AKA Android internal bug 33393474.	Version(s): Google Android 7.1.1 and earlier before 2017-03-05 on Pixel C, Pixel, and Pixel XL	Published - March 06, 2017 CVE-2016-9806 CVSS - 9.3 Vendor's Advisory Available at : http://source.android.com/security/bulletin/2017-03-01.html
Google Android 7.1.1 and Earlier Unspecified Vulnerability in a Qualcomm Component	Google Android 7.1.1 and earlier, before 2017-03-05, is prone to a critical unspecified vulnerability in a Qualcomm component. AKA Android internal bug 28823681.	Version(s): Google Android 7.1.1 and earlier, before 2017-03-05.	Published - March 05, 2017 CVE-2016-8485 CVSS - 9.3 Vendor's Advisory Available at: https://source.android.com/security/bulletin/2017-03-01.html