PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
SAP NetWeaver UDDI Server Remote Code Execution Vulnerability - CVE-2019-0351	A remote code execution vulnerability exists in the SAP NetWeaver UDDI Server (Services Registry), versions 7.10, 7.20, 7.30, 7.31, 7.40, and 7.50. Because of this, an attacker can exploit Services Registry potentially enabling them to take complete control of the product, including viewing, changing, or deleting data by injecting code into the working memory which is subsequently executed by the application. It can also be used to cause a general fault in the product, causing the product to terminate.	Business Version 7.40, 7.50, 7.20, 7.31, 7.30, 7.10	Vendor - SAP CVE Id - CVE-2019-0351 CVSS Base - 9.9 Reporting Date - 08/13/2019 Vendor's Advisory - https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=523998017
Adobe Acrobat and Reader Remote Code Execution Vulnerability due to Out-of-Bounds Write - CVE-2019-7965	Acrobat DC Continuous through 2019.012.20035, Acrobat Reader DC Continuous through 2019.012.20035, Acrobat 2017 Classic through 2017.011.30143, Acrobat Reader 2017 Classic through 2017.011.30138, Acrobat DC Classic through 2015.006.30498 and Acrobat Reader DC through 2015.006.30498 are prone to arbitrary code execution due to an out-of-bounds write.	Reader 2017 <=2017.011.30143, <=2017.011.30142 Acrobat 2017 <=2017.011.30143, <=2017.011.30142 Acrobat DC Continuous <=2019.012.20035, <=2019.012.20034 Reader DC Continuous <=2019.012.20035, <=2019.012.20034 Reader DC Classic <=2017.11.30497, <=2017.011.30498 Acrobat DC Classic <=2017.006.30497, <=2017.006.30498	Vendor - Adobe CVE Id - CVE-2019-7965 CVSS Base - 9.8 Reporting Date - 08/21/2019 Vendor's Advisory - https://helpx.adobe.com/security/products/acrobat/apsb19-41.html
Adobe Creative Cloud Desktop Application <4.9 Privilege Escalation Vulnerability - CVE-2019-7958,CVE-2019-7959	Adobe Creative Cloud Desktop Application 4.6.1 and earlier is prone to a privilege escalation vulnerability of critical severity due to insecure inherited permissions issue.	Creative Cloud <=4.6.1	Vendor - Adobe CVE Id - CVE-2019-7958, CVE-2019-7959 CVSS Base - 9.8 Reporting Date - 08/13/2019 Vendor's Advisory - https://helpx.adobe.com/security/products/acrobat/apsb19-39.html
Adobe Photoshop CC 19 before 19.1.9 and 20 before 20.0.6 Remote Code Execution due to Command Injection - CVE-2019-7968	Adobe Photoshop CC 19 before 19.1.9 and 20 before 20.0.6 on Windows and MacOS is prone to a critical remote code execution vulnerability due to a command injection issue.	Photoshop 20.0 - 20.0.5, 19.0 - 19.1.8	Vendor - Adobe CVE Id - CVE-2019-7968 CVSS Base - 9.8 Reporting Date - 08/13/2019 Vendor's Advisory - https://helpx.adobe.com/security/products/acrobat/apsb19-44.html
Cisco Webex and IP Phones Local Network Key Negotiation of Bluetooth Vulnerability - CVE-2019-9506 ("KNOB")	Cisco Webex DX70 and DX80, Cisco 8821 Wireless IP Phones, Cisco 8845 IP Phones, Cisco 8851 IP Phones, Cisco 8861 IP Phones, Cisco 8865 IP Phones, and Cisco SPA525G2 Small Business IP Phones are affected by a vulnerability in the Bluetooth BR/EDR specification. An attacker could potentially be able to negotiate the offered key length down to 1 byte of entropy, from a maximum of 16 bytes.This allows practical brute-force attacks (aka "KNOB") that can decrypt traffic and inject arbitrary ciphertext without the victim noticing.	IP Phone 8800 = 8861, 8821, 8865, 8845 WebEx DX Series = DX80, DX70 SPA525 Series IP Phone HW = SPA525G2	Vendor - Cisco CVE Id - CVE-2019-9506 CVSS Base - 9.8 Reporting Date - 08/13/2019 Vendor's Advisory - http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190813-bluetooth
Ghostscript Remote Code Execution and Information Disclosure Vulnerability - CVE-2019-10216	Ghostscript up to and including 9.27 is prone to a code execution and information disclosure vulnerability due to a bypass of the ghostscript sandbox.	Enterprise Linux Server 7, EUS 7.7, TUS 7.7, AUS 7.7 Enterprise Linux Workstation 7 Ghostscript <9.29	Vendor - Artifex Software and RedHat CVE Id - CVE-2019-10216 CVSS Base - 9.8 Reporting Date - 08/13/2019 Vendor's Advisory - http://rhn.redhat.com/errata/RHSA-2019-2465.html
Microsoft Outlook Elevation of Privilege Vulnerability - CVE-2019-1204	Microsoft Office 2019, Outlook 2010 SP2, 2013 RT SP1, and 2016, and Office 365 ProPlus are vulnerable to an elevation of privileges vulnerability when Outlook initiates processing of incoming messages without sufficient validation of the formatting of the messages. A remote attacker could exploit this issue to force Outlook to load a local or remote message store (over SMB).	Office 365 ProPlus X64, ProPlus X86 Office 2019 X64, 2019X86 Outlook 2013 SP1RP, 2016 X64, 2016 X86, 2010 SP2 X86, 2010 SP2 x86, 2013 SP1 x64, 2013 SP1 x86	Vendor - Microsoft CVE Id - CVE-2019-1204 CVSS Base - 9.8 Reporting Date - 08/13/2019 Vendor's Advisory - https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-1204
Microsoft Encryption Key Negotiation of Bluetooth Vulnerability - CVE-2019-9506 ("KNOB")	Microsoft Windows versions may be affected by the bluetooth BR/EDR (basic rate/enhanced data rate, aka "Bluetooth Classic") key negotiation vulnerability that exists at the hardware specification level of BR/EDR Bluetooth devices. An attacker could potentially be able to negotiate the offered key length down to 1 byte of entropy, from a maximum of 16 bytes. To address the vulnerability Microsoft released a software update that enforces a default 7-octet minimum key length. This functionality is disabled by default when the update is installed. Customers need to enable the functionality by setting a flag in the registry. Affected versions are: Windows 10, Windows 10 Version 1607 , Windows 10 Version 1703, Windows 10 Version 1709, Windows 10 Version 1803, Windows 10 Version 1809, Windows 10 Version 1903, Windows 7, Windows 8.1, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server version 1803 and Windows Server version 1903.	Windows Server 2019 Windows Server 2008 R2 Windows 7 Windows 8 Windows 10 Windows Server Windows Server 2016 Windows Server 2012 Windows Server 2012 R2	Vendor - Microsoft CVE Id - CVE-2019-9506 CVSS Base - 9.8 Reporting Date - 08/13/2019 Vendor's Advisory - https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-9506
Microsoft Guidance for Enabling LDAP Channel Binding and LDAP Signing (ADV190023)	Microsoft has published an advisory regarding how to mitigate the effect of unsafe default configurations for LDAP channel binding and LDAP signing on Active Directory Domain Controllers. These configurations could enable LDAP clients to communicate without enforcing LDAP channel binding and LDAP signing. The instructions are published in Knowledge Base articles KB4034879 and KB935834. This vulnerability was published by Microsoft	Active Directory	Vendor - Microsoft CVE Id - CVE-2019-9506 CVSS Base - 9.8 Reporting Date - 08/13/2019 Vendor's Advisory - https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190023
SAP Kernel Missing Authorization Check Vulnerability - CVE-2019-0349	SAP Kernel (ABAP Debugger), versions KRNL32NUC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL32UC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL64NUC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, KRNL64UC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, 7.73, KERNEL 7.21, 7.49, 7.53, 7.73, 7.75, 7.76, 7.77, allows a user to execute ?Go to statement? without possessing the authorization S_DEVELOP DEBUG 02, resulting in Missing Authorization Check.	SAP Kernell 7.22EXT, 7.49, 7.21EXT, 7.73, 7.53, 7.22, 7.77, 7.21, 7.76	Vendor - SAP CVE Id - CVE-2019-0349 CVSS Base - 9.8 Reporting Date - 08/13/2019 Vendor's Advisory - https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=523998017
Adobe Experience Manager Remote Code Execution Vulnerability - CVE-2019-7964	Adobe Experience Manager versions 6.4 and 6.5 are prone to a code execution vulnerability due to an authentication bypass.	Experience Manager 6.4, 6.5	Vendor - Adobe CVE Id - CVE-2019-7964 CVSS Base - 9.8 Reporting Date - 08/13/2019 Vendor's Advisory - https://helpx.adobe.com/security/products/experience-manager/apsb19-42.html
IBM WebSphere Application Server Local Privilege Escalation Vulnerability in Java - CVE-2019-11771, CVE-2019-4473	Multiple binaries in IBM Java 7, 7R1 and 8 , as used in IBM WebSphere Application Server Liberty 16.0.0.2 through 19.0.0.7, and IBM WebSphere Application Server and Application Client for IBM WebSphere Application Server 8.5.0.0 through 8.5.5.15, and 9.0.0.0 through 9.0.5.0 on the AIX platform use insecure absolute RPATHs, which may facilitate code injection and privilege elevation by local users. IBM X-Force ID: 163984.	Application client for IBM WebSphere 8.5.0.0-8.5.5.15, 9.0.0.0 - 9.0.5.0 Application client for IBM Server 8.5.0.0-8.5.5.15, 9.0.0.0 - 9.0.5.0 WebSphere Application Server Library 16.0.02 - 19.0.07	Vendor - IBM CVE Id - CVE-2019-4473, CVE-2019-11771 CVSS Base - 8.4 Reporting Date - 08/22/2019 Vendor's Advisory - https://www-01.ibm.com/support/docview.wss?uid=ibm10964780&myns=swgws&mynp=OCSSEQTP&mync=E&cm_sp=swgws-_-OCSSEQTP-_-E

PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Cisco Integrated Management Controller Supervisor, Cisco UCS Director, Cisco UCS Director Express for Big Data Remote Code Execution Vulnerability - CVE-2019-1935, CVE-2019-1937, CVE-2019-1974, CVE-2019-1938	A vulnerability in Cisco Integrated Management Controller (IMC) Supervisor, Cisco UCS Director, and Cisco UCS Director Express for Big Data could allow an unauthenticated, remote attacker to log in to the CLI of an affected system by using the SCP User account (scpuser), which has default user credentials. The vulnerability is due to the presence of a documented default account with an undocumented default password and incorrect permission settings for that account. Changing the default password for this account is not enforced during the installation of the product. An attacker could exploit this vulnerability by using the account to log in to an affected system. A successful exploit could allow the attacker to execute arbitrary commands with the privileges of the scpuser account. This includes full read and write access to the system's database.	UCS Directo 6.5*, 6.7.1.0,6.0*, 6.6.0.0, 6.6.1.0, 6.7.0.0 Integrated Management Controller supervisor 2.2.0.2 - 2.2.0.6, 2.1* UCS Director Express for Big Data 3.5.*, 3.6.*, 3.6.0.0, 3.0.*, 3.7.1.0, 3.7.0.0, 3.6.1.0	Vendor - CISCO CVE Id - CVE-2019-1935, CVE-2019-1937, CVE-2019-1974, CVE-2019-1938 CVSS Base - 9.8 Reporting Date - 08/21/2019 Vendor's Advisory - http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imcs-usercred
Linux kernel <5.0.10 Remote Use-After-Free Vulnerability - CVE-2019-15214	An issue was discovered in the Linux kernel before 5.0.10. There is a use-after-free in the sound subsystem because card disconnection causes certain data structures to be deleted too early. This is related to sound/core/init.c and sound/core/info.c.	Linux Kernel <5.0.10	Vendor - Linux CVE Id - CVE-2019-15214 CVSS Base - 9.8 Reporting Date - 08/19/2019 Vendor's Advisory - https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=8c2f870890fd28e023b0fcf49dcee333f2c8bad7
Linux kernel <5.2.6 Remote Use-After-Free Vulnerability - CVE-2019-15211, CVE-2019-15215	An issue was discovered in the Linux kernel before 5.2.6. There is a use-after-free caused by a malicious USB device in the drivers/media/v4l2-core/v4l2-dev.c driver because drivers/media/radio/radio-raremono.c does not properly allocate memory.	Linux Kernel <5.2.6	Vendor - Linux CVE Id - CVE-2019-15211, CVE-2019-15215 CVSS Base - 9.8 Reporting Date - 08/19/2019 Vendor's Advisory - https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.2.6