

Histórico de vulnerabilidades de Abril do 2016

Semana 11/04/2016				
Primary Vendor - Product	Description	Published	CVSS Score	Source & Patch Info
Google-android	Stack-based buffer overflow in decoder/ffmpeg_vid.c in mediaserver in Android 6.x before 2016-04-01 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 25812590.	17/04/2016	10.0	CVE-2016-0936
Cisco-unified	Heap-based buffer overflow in Cisco Unified Computing System (UCS) Platform Emulator 2.5(2)T54, 3.0(2)X4, and 3.0(2)T59 allows local users to gain privileges via crafted libicmtr.so filename arguments. aka Bug ID CSCuc68837.	15/04/2016	7.2	CVE-2016-1340
Cisco-unified	Cisco Unified Computing System (UCS) Platform Emulator 2.5(2)T54, 3.0(2)X4, and 3.0(2)T59 allows local users to gain privileges via crafted arguments on a process-exec command line. aka Bug ID CSCuc68837.	15/04/2016	7.2	CVE-2016-1339
Juniper-screens	The administrative web services interface in Juniper ScreenOS before 6.3.0r21 allows remote attackers to cause a denial of service (reboot) via a crafted SSL packet.	15/04/2016	7.8	CVE-2016-1348
Sap-netweaver	XML external entity (XXE) vulnerability in the UDDI component in SAP NetWeaver JAVA AS 7.4 allows remote attackers to cause a denial of service via a crafted XML entity. aka SAP Security Note 295-6380.	14/04/2016	9.0	CVE-2016-4014
Apache-subversion	Integer overflow in util.c in mod_ajk in Apache Subversion 1.7.4, 1.x before 1.8.15, and 1.9.x before 1.9.3 allows remote authenticated users to cause a denial of service (subversion server crash or memory consumption) and possibly execute arbitrary code via a skel-encoded request body, which triggers an out-of-bounds read and heap-based buffer overflow.	14/04/2016	8.0	CVE-2015-5343
Debian-linux	Heap-based buffer overflow in the bmp_read_rows function in pngbmp.c in CgPNG before 0.7.6 allows remote attackers to cause a denial of service (out-of-bounds read or write access and crash) or possibly execute arbitrary code via a crafted image file.	13/04/2016	9.3	CVE-2016-3961
Huawei-mate	Integer overflow in the graphics drivers in Huawei Mate 5 smartphones with software CRB-TL00 before CRB-TL00C01B16GSP01, CRB-UL00 before CRB-UL00C00B160, and CRB-CL00 before CRB-CL00C92B161 allows attackers to cause a denial of service (system crash) or gain privileges via a crafted application, which triggers a heap-based buffer overflow.	13/04/2016	9.1	CVE-2016-1495
Avast-freeantivirus	Heap-based buffer overflow in the Avast virtualization driver (asw5m.sys) in Avast Internet Security, Pro Antivirus, Premier, and Free Antivirus before 11.1.2253 allows local users to gain privileges via a Unicode file path in an IOCTL request.	13/04/2016	10.0	CVE-2015-8620
Huawei-p7	Integer overflow in Huawei P7 phones with software before P7-L07 V100R001C01B606 allows remote attackers to gain privileges via a crafted application with the system or camera permission.	13/04/2016	9.3	CVE-2015-8304
Microsoft-windows	The kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-0143 and CVE-2016-0165.	12/04/2016	7.2	CVE-2016-0167
Microsoft-internetexplorer	Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site. aka "Internet Explorer Memory Corruption Vulnerability."	12/04/2016	7.6	CVE-2016-0166
Microsoft-windows	The kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-0143 and CVE-2016-0167.	12/04/2016	7.2	CVE-2016-0165
Microsoft-internetexplorer	Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site. aka "Internet Explorer Memory Corruption Vulnerability."	12/04/2016	7.6	CVE-2016-0164
Microsoft-internetexplorer	Microsoft Internet Explorer 11 mishandles DLL loading, which allows local users to gain privileges via a crafted application, aka "DLL Loading Remote Code Execution Vulnerability."	12/04/2016	7.2	CVE-2016-0160
Microsoft-internetexplorer	Microsoft Internet Explorer 9 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site. aka "Internet Explorer Memory Corruption Vulnerability."	12/04/2016	7.6	CVE-2016-0159
Microsoft-edge	Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0155 and CVE-2016-0156.	12/04/2016	7.6	CVE-2016-0157
Microsoft-edge	Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0155 and CVE-2016-0157.	12/04/2016	7.6	CVE-2016-0156
Microsoft-edge	Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0156 and CVE-2016-0157.	12/04/2016	7.6	CVE-2016-0155
Microsoft-edge	Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability."	12/04/2016	7.6	CVE-2016-0154
Microsoft-windows	OLE in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT 8.1 allows remote attackers to execute arbitrary code via a crafted file, aka "Windows OLE Remote Code Execution Vulnerability."	12/04/2016	9.3	CVE-2016-0153
Microsoft-windows	The Client Server Run-time Subsystem (CSRSS) in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 mismanages process tokens, which allows local users to gain privileges via a crafted application, aka "Windows CSRSS Security Feature Bypass Vulnerability."	12/04/2016	7.2	CVE-2016-0151
Microsoft-windows	HTTP.sys in Microsoft Windows 10 Gold and 1511 allows remote attackers to cause a denial of service (system hang) via crafted HTTP 3.0 requests. aka "HTTP.sys Denial of Service Vulnerability."	12/04/2016	7.8	CVE-2016-0150
Microsoft-netframework	Microsoft .NET Framework 4.6 and 4.6.1 mishandles library loading, which allows local users to gain privileges via a crafted application, aka ".NET Framework Remote Code Execution Vulnerability."	12/04/2016	7.4	CVE-2016-0148
Microsoft-xml	Microsoft XML Core Services 3.0 allows remote attackers to execute arbitrary code via a crafted web site, aka "MSXML 3.0 Remote Code Execution Vulnerability."	12/04/2016	9.3	CVE-2016-0147
Microsoft-five	The font library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold and 1511, Office 2007 SP3 and 2010 SP2, Word Viewer, .NET Framework 3.0 SP2, 3.5, and 3.5.1, Skype for Business 2016, Lync 2010, Lync 2010 Attendee, Lync 2013 SP1, and Live Meeting 2007 Console allows remote attackers to execute arbitrary code via a crafted embedded font, aka "Graphics Memory Corruption Vulnerability."	12/04/2016	9.1	CVE-2016-0145
Microsoft-windows	The kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-0143 and CVE-2016-0167.	12/04/2016	7.2	CVE-2016-0143
Microsoft-excel	Microsoft Excel 2007 SP3, Word for Mac 2011, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	12/04/2016	9.3	CVE-2016-0139
Microsoft-sharepoint	Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Compatibility Pack SP3, Excel Services on SharePoint Server 2007 SP3, and Excel Services on SharePoint Server 2010 SP2 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	12/04/2016	9.3	CVE-2016-0136
Microsoft-windows	The Secondary Logon Service in Microsoft Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka "Secondary Logon Elevation of Privilege Vulnerability."	12/04/2016	7.2	CVE-2016-0135
Microsoft-office	Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Office Compatibility Pack SP3, Word Viewer, Word Automation Services on SharePoint Server 2010 SP2, Word Automation Services on SharePoint Server 2013 SP1, Office Web Apps 2010 SP2, and Office Web Apps Server 2013 SP1 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	12/04/2016	9.3	CVE-2016-0127
Microsoft-excel	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Word 2016 for Mac, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	12/04/2016	9.3	CVE-2016-0122
Huawei-policy	Huawei Policy Center with software before V100R003C05P0020 allows remote authenticated users to gain privileges and cause a denial of service (system crash) via a crafted URL.	12/04/2016	9.0	CVE-2016-2405
Apache-struts	Apache Struts 2.x before 2.3.28 allows remote attackers to execute arbitrary code via a "60)" sequence in a tag attribute, aka forced double DOCTYPE evaluation.	12/04/2016	10.0	CVE-2016-0785
Microsoft-windows	The Escape interface in the Kernel Mode Driver layer in the NVIDIA GPU graphics driver R304 before 341.95 and R352 before 354.74 on Windows improperly allows access to restricted functionality, which allows local users to gain privileges via unspecified vectors.	12/04/2016	7.2	CVE-2016-2556
Avast	Avast allows remote attackers to cause a denial of service (memory corruption) and possibly execute arbitrary code via a crafted PE file, related to authenticode parsing.	11/04/2016	9.1	CVE-2016-3986
Qemu	Use-after-free vulnerability in hw/ide/ahci.c in QEMU, when built with IDE AHCI Emulation support, allows guest OS users to cause a denial of service (instance crash) or possibly execute arbitrary code via an invalid AHCI Native Command Queuing (NCQ) AIO command.	11/04/2016	9.1	CVE-2016-1568
Claws-mail	Stack-based buffer overflow in the conv_eucjis function in codecov.c in Claws Mail 3.13.1 allows remote attackers to have unspecified impact via a crafted email, involving Japanese character set conversion. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-8614.	11/04/2016	7.5	CVE-2015-8708
Apache-directory	The CSV export in Apache LDAP Studio and Apache Directory Studio before 2.0.0-M10 does not properly escape field values, which might allow attackers to execute arbitrary commands by leveraging a crafted LDAP entry that is interpreted as a formula when imported into a spreadsheet.	11/04/2016	9.3	CVE-2015-5349
Redhat-openstack	The TripleO Heat templates (tripleo-heat-templates), as used in Red Hat Enterprise Linux OpenStack Platform 7.0, do not properly use the configured RabbitMQ credentials, which makes it easier for remote attackers to obtain access to services in deployed overclouds by leveraging knowledge of the default credentials.	11/04/2016	7.5	CVE-2015-5320
Lenovo-fingerprint	Lenovo Fingerprint Manager before 8.01.57 and Touch Fingerprint before 1.00.08 use weak ACLs for unspecified (1) services and (2) files, which allows local users to gain privileges by invalidating local checks.	11/04/2016	7.2	CVE-2016-2393

Semana 04/04/2016				
Primary Vendor - Product	Description	Published	CVSS Score	Source & Patch Info
Adobe-flash-player	Stack-based buffer overflow in Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code via crafted JPEG-R8 data.	08/04/2016	9.3	CVE-2016-1018
Adobe-flash-player	Use-after-free vulnerability in the LoadVars.decode function in Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1011, CVE-2016-1013, CVE-2016-1016, and CVE-2016-1031.	08/04/2016	9.3	CVE-2016-1017
Microsoft-windows10	Use-after-free vulnerability in the Transform object implementation in Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code via a flash.geom.Matrix callback, a different vulnerability than CVE-2016-1011, CVE-2016-1013, CVE-2016-1017, and CVE-2016-1031.	08/04/2016	9.3	CVE-2016-1016
Microsoft-windows8,1	Untrusted search path vulnerability in Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows local users to gain privileges via a Trojan horse resource in an unspecified directory.	08/04/2016	7.2	CVE-2016-1014
Rubyonrails-ruby	Action Pack in Ruby on Rails before 3.2.22.2, 4.x before 4.1.14.2, and 4.2.x before 4.2.5.2 allows remote attackers to execute arbitrary Ruby code by leveraging an application's unrestricted use of the render method.	07/04/2016	7.5	CVE-2016-2098
cloudbees-jenkins	Multiple unspecified API endpoints in Cloudbees Jenkins before 1.650 and LTS before 1.642.2 allow remote authenticated users to execute arbitrary code via serialized data in an XML file, related to XStream and groovy.util.Expando.	07/04/2016	9.0	CVE-2016-0792
Huawei-mate	The ovtp driver in Huawei P8 smartphones with software GRA-TL00 before GRA-TL00C01B230, GRA-CL00 before GRA-CL00C92B230, GRA-UL00 before GRA-UL00C92B230, GRA-UL00 before GRA-UL00C00B230, and GRA-UL00 before GRA-UL00C00B230, and Mate 5 smartphones with software CRB-TL00 before CRB-TL00C01B16GSP01, CRB-UL00 before CRB-UL00C00B160, and CRB-CL00 before CRB-CL00C92B161 allows attackers to cause a denial of service (system crash) or gain privileges via a crafted application with the camera permission, aka an "interface access control vulnerability."	07/04/2016	9.1	CVE-2015-8661
Huawei-p8	The Graphics driver in Huawei P8 smartphones with software GRA-TL00 before GRA-TL00C01B230, GRA-CL00 before GRA-CL00C92B230, GRA-UL00 before GRA-UL00C92B230, GRA-UL00 before GRA-UL00C00B230, and GRA-UL00 before GRA-UL00C00B230, and Mate 5 smartphones with software CRB-TL00 before CRB-TL00C01B16GSP01, CRB-UL00 before CRB-UL00C00B160, and CRB-CL00 before CRB-CL00C92B161 allows attackers to cause a denial of service (system crash) or gain privileges via a crafted application with the graphics permission, aka an "interface access control vulnerability," a different vulnerability than CVE-2015-8307.	07/04/2016	9.1	CVE-2015-8660
Huawei-mate	Heap-based buffer overflow in the HFI driver in Huawei P8 smartphones with software GRA-TL00 before GRA-TL00C01B230, GRA-CL00 before GRA-CL00C92B230, GRA-UL00 before GRA-UL00C92B230, GRA-UL00 before GRA-UL00C00B230, and GRA-UL00 before GRA-UL00C00B230, and Mate 5 smartphones with software CRB-TL00 before CRB-TL00C01B16GSP01, CRB-UL00 before CRB-UL00C00B160, and CRB-CL00 before CRB-CL00C92B161 allows attackers to cause a denial of service (system crash) or gain privileges via a crafted application, a different vulnerability than CVE-2015-8318.	07/04/2016	9.1	CVE-2015-8319

Histórico de vulnerabilidades de Abril do 2016

Primary Vendor – Product	Description	Published	CVSS Score	Source & Patch Info
Huawei–mate	Heap-based buffer overflow in the HFI driver in Huawei P8 smartphones with software GRA-TL00 before GRA-TL00C01B230, GRA-CL00 before GRA-CL00C02B230, GRA-CL10 before GRA-CL10C02B230, GRA-UL00 before GRA-UL00C00B230, and GRA-UL10 before GRA-UL10C00B230, and Mate S smartphones with software CRR-TL00 before CRR-TL00C01B160SPO1, CRR-UL00 before CRR-UL00C00B160, and CRR-CL00 before CRR-CL00C02B161 allows attackers to cause a denial of service (system crash) or gain privileges via a crafted application, a different vulnerability than CVE-2015-8319.	07/04/2016	9.3	CVE-2015-8318
Huawei–mate	The Graphics driver in Huawei P8 smartphones with software GRA-TL00 before GRA-TL00C01B230, GRA-CL00 before GRA-CL00C02B230, GRA-CL10 before GRA-CL10C02B230, and Mate S smartphones with software CRR-TL00 before CRR-TL00C01B160SPO1, CRR-UL00 before CRR-UL00C00B160, and CRR-CL00 before CRR-CL00C02B161 allows attackers to cause a denial of service (system crash) or gain privileges via a crafted application with the graphics permission, aka an "interface access control vulnerability," a different vulnerability than CVE-2015-8680.	07/04/2016	9.3	CVE-2015-8307
Sap-netweaver	XML external entity (XXE) vulnerability in the Configuration Wizard in SAP NetWeaver Java AS 7.4 allows remote attackers to cause a denial of service, conduct SMB Relay attacks, or access arbitrary files via a crafted XML request, related to the ctp:protocol servlet, aka SAP Security Note 2235994.	07/04/2016	7.5	CVE-2016-3974
Squid–cache	Heap-based buffer overflow in the icmp6_recv function in icmp/icmp6.cc in the pinger in Squid before 3.5.16 and 4.x before 4.0.8 allows remote servers to cause a denial of service (performance degradation or transition failures) or write sensitive information to log files via an ICMPv6 packet.	07/04/2016	7.5	CVE-2016-3947
Adobe–flashplayer	Adobe Flash Player 21.0.0.197 and earlier allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via unspecified vectors, as exploited in the wild in April 2016.	07/04/2016	10.0	CVE-2016-1029
Emc–documentum	EMC Documentum D2 before 4.6 lacks intended ACLs for configuration objects, which allows remote authenticated users to modify objects via unspecified vectors.	07/04/2016	9.0	CVE-2016-0888
Cisco–telepresence	The kernel in Cisco TelePresence Server 3.0 through 4.2(4.18) on Mobility Services Engine (MSE) 8710 devices allows remote attackers to cause a denial of service (panic and reboot) via a crafted sequence of IPv6 packets, aka Bug ID CSCu46673.	06/04/2016	7.1	CVE-2016-1346
Cisco–ucs	Cisco UCS Invicta C3124SA Appliance 4.3.1 through 5.0.1, UCS Invicta Scaling System and Appliance, and Whiplash Racerunner improperly store a default SSH private key, which allows remote attackers to obtain root access via unspecified vectors, aka Bug ID CSCu71294.	06/04/2016	10.0	CVE-2016-1313
Cisco–evolved	Cisco Prime Infrastructure 1.2.0 through 2.2(2) and Cisco Evolved Programmable Network Manager (EPNM) 1.2 allow remote attackers to execute arbitrary code via crafted deserialized data in an HTTP POST request, aka Bug ID CSCu63192.	06/04/2016	9.3	CVE-2016-1291
Cisco–telepresence	Cisco TelePresence Server 4.1(2.29) through 4.2(4.17) on 7010; Mobility Services Engine (MSE) 8710; Multiparty Media 310, 320, and 820; and Virtual Machine (VM) devices allows remote attackers to cause a denial of service (memory consumption or device reload) via crafted HTTP requests that are not followed by an unspecified negotiation, aka Bug ID CSCu47565.	06/04/2016	7.8	CVE-2015-6313
Cisco–telepresence	Cisco TelePresence Server 3.1 on 7010; Mobility Services Engine (MSE) 8710; Multiparty Media 310 and 320; and Virtual Machine (VM) devices allows remote attackers to cause a denial of service (device reload) via malformed STUN packets, aka Bug ID CSCu01348.	06/04/2016	7.8	CVE-2015-6312
Fedora–project	The mod_tls module in ProFTPD before 1.3.5b and 1.3.6 before 1.3.6rc2 does not properly handle the TLSDHParamFile directive, which might cause a weaker than intended Diffie-Hellman (DH) key to be used and consequently allow attackers to have unspecified impact via unknown vectors.	05/04/2016	10.0	CVE-2016-3125
Hp–asset	HP Asset Manager 9.40, 9.41, and 9.50 and Asset Manager CloudSystem ChargeBack 9.40 allow remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the Apache Commons Collections (ACC) library.	05/04/2016	7.5	CVE-2016-2000
Ibm-tivoli	Buffer overflow in the server in IBM Tivoli Storage Manager FastBack 5.5.x and 6.x before 6.1.12.2 allows remote attackers to execute arbitrary code via a crafted command, a different vulnerability than CVE-2015-8515, CVE-2015-8520, and CVE-2015-8521.	05/04/2016	7.5	CVE-2015-8522
Ibm-tivoli	Buffer overflow in the server in IBM Tivoli Storage Manager FastBack 5.5.x and 6.x before 6.1.12.2 allows remote attackers to execute arbitrary code via a crafted command, a different vulnerability than CVE-2015-8519, CVE-2015-8520, and CVE-2015-8522.	05/04/2016	7.5	CVE-2015-8521
Ibm-tivoli	Buffer overflow in the server in IBM Tivoli Storage Manager FastBack 5.5.x and 6.x before 6.1.12.2 allows remote attackers to execute arbitrary code via a crafted command, a different vulnerability than CVE-2015-8519, CVE-2015-8521, and CVE-2015-8522.	05/04/2016	7.5	CVE-2015-8520
Ibm-tivoli	Buffer overflow in the server in IBM Tivoli Storage Manager FastBack 5.5.x and 6.x before 6.1.12.2 allows remote attackers to execute arbitrary code via a crafted command, a different vulnerability than CVE-2015-8620, CVE-2015-8521, and CVE-2015-8522.	05/04/2016	7.5	CVE-2015-8519
Patterson–dental	Patterson Dental Eaglesoft 17 has a hardcoded password for sql for the dba account, which allows remote attackers to obtain sensitive Dental DB patient information via SQL statements.	01/04/2016	10.0	CVE-2016-2343