

05.04.2022

DIVISIÓN DE REDES Y SEGURIDAD INFORMÁTICA

DEPARTAMENTO CSIRT

Vulnerabilidades que requieren parchado urgente según la CISA de Estados Unidos

La Agencia de Ciberseguridad e Infraestructura (CISA) del Gobierno Federal de los Estados Unidos mantiene y actualiza frecuentemente una lista de las vulnerabilidades más importantes que están siendo explotadas en el ciberespacio de dicho país.

Consideramos que este listado (disponible en <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>) supone un material útil para difundir también en Chile, ya que muchos de los sistemas que se usan en nuestro país son los mismos afectados por las vulnerabilidades destacadas por la CISA

Actualmente, el listado está compuesto de las siguientes 609 vulnerabilidades, **que recomendamos parchar cuanto antes, usando las actualizaciones dispuestas por los respectivos proveedores en sus sitios web.**

Una excepción son las siguientes vulnerabilidades, en cuyos casos la CISA recomienda desconectar los productos porque ya están fuera del período de respaldo de sus proveedores:

CVE	Proveedor	Productos afectados
CVE-2015-2051	D-Link	DIR-645 Router
CVE-2020-9377	D-Link	DIR-610 Devices
CVE-2019-16920	D-Link	Multiple Routers
CVE-2017-6334	NETGEAR	DGN2200 Devices
CVE-2016-7892	Adobe	Flash Player
CVE-2016-4171	Adobe	Flash Player
CVE-2016-11021	D-Link	DCS-930L Devices
CVE-2015-1187	D-Link and TRENDnet	Multiple Devices
CVE-2021-20028	SonicWall	Secure Remote Access (SRA)
CVE-2018-10562	Dasan	Gigabit Passive Optical Network (GPON) Routers
CVE-2018-10561	Dasan	Gigabit Passive Optical Network (GPON) Routers
CVE-2021-45382	D-Link	Multiple Routers

Listado de vulnerabilidades

CVE	Proveedor	Productos afectados	Vulnerabilidad
CVE-2021-27104	Accellion	FTA	Accellion FTA OS Command Injection Vulnerability
CVE-2021-27102	Accellion	FTA	Accellion FTA OS Command Injection Vulnerability
CVE-2021-27101	Accellion	FTA	Accellion FTA SQL Injection Vulnerability
CVE-2021-27103	Accellion	FTA	Accellion FTA SSRF Vulnerability
CVE-2021-21017	Adobe	Acrobat and Reader	Adobe Acrobat and Reader Heap-based Buffer Overflow Vulnerability
CVE-2021-28550	Adobe	Acrobat and Reader	Adobe Acrobat and Reader Use-After-Free Vulnerability
CVE-2018-4939	Adobe	ColdFusion	Adobe ColdFusion Deserialization of Untrusted Data vulnerability
CVE-2018-15961	Adobe	ColdFusion	Adobe ColdFusion Remote Code Execution
CVE-2018-4878	Adobe	Flash Player	Adobe Flash Player Use-After-Free vulnerability
CVE-2020-5735	Amcrest	Cameras and Network Video Recorder (NVR)	Amcrest Camera and NVR Buffer Overflow Vulnerability
CVE-2019-2215	Android	Android OS	Android "AbstractEmu" Root Access Vulnerabilities
CVE-2020-0041	Android	Android OS	Android "AbstractEmu" Root Access Vulnerabilities
CVE-2020-0069	Android	Android OS	Android "AbstractEmu" Root Access Vulnerabilities
CVE-2017-9805	Apache	Struts	Apache Struts Multiple Versions Remote Code Execution Vulnerability
CVE-2021-42013	Apache	HTTP Server	Apache HTTP Server 2.4.49 and 2.4.50 Path Traversal
CVE-2021-41773	Apache	HTTP Server	Apache HTTP Server Path Traversal Vulnerability
CVE-2019-0211	Apache	HTTP Server	Apache HTTP Server scoreboard vulnerability
CVE-2016-4437	Apache	Shiro	Apache Shiro 1.2.4 Cookie RememberME Deserial Remote Code Execution Vulnerability
CVE-2019-17558	Apache	Solr	Apache Solr 5.0.0-8.3.1 Remote Code Execution Vulnerability
CVE-2020-17530	Apache	Struts	Apache Struts Forced OGNL Double Evaluation Remote Code Execution

CVE-2017-5638	Apache	Struts	Apache Struts Jakarta Multipart parser exception handling vulnerability
CVE-2018-11776	Apache	Struts	Apache Struts 2.3 to 2.3.34 and 2.5 to 2.5.16 Remote Code Execution Vulnerability
CVE-2021-30858	Apple	iOS and iPadOS	Apple Apple iOS and iPadOS Use-After-Free Vulnerability
CVE-2019-6223	Apple	FaceTime	Apple FaceTime Vulnerability
CVE-2021-30860	Apple	iOS	Apple iOS "FORCEDENTRY" Remote Code Execution Vulnerability
CVE-2020-27930	Apple	iOS and macOS	Apple iOS and macOS FontParser Remote Code Execution Vulnerability
CVE-2021-30807	Apple	iOS and macOS	Apple iOS and macOS Memory Corruption Vulnerability
CVE-2020-27950	Apple	iOS and macOS	Apple iOS and macOS Kernel Memory Initialization Vulnerability
CVE-2020-27932	Apple	iOS and macOS	Apple iOS and macOS Kernel Type Confusion Vulnerability
CVE-2020-9818	Apple	iOS Mail	Apple iOS Mail OOB Vulnerability
CVE-2020-9819	Apple	iOS Mail	Apple iOS Mail Heap Overflow Vulnerability
CVE-2021-30762	Apple	iOS	Apple WebKit Browser Engine Use-After-Free Vulnerability
CVE-2021-1782	Apple	iOS	Apple iOS Privilege Escalation and Code Execution Chain
CVE-2021-1870	Apple	iOS	Apple iOS Privilege Escalation and Code Execution Chain
CVE-2021-1871	Apple	iOS	Apple iOS Privilege Escalation and Code Execution Chain
CVE-2021-1879	Apple	iOS	Apple iOS Webkit Browser Engine XSS
CVE-2021-30661	Apple	iOS	Apple iOS Webkit Storage Use-After-Free Remote Code Execution Vulnerability
CVE-2021-30666	Apple	iOS	Apple iOS12.x Buffer Overflow
CVE-2021-30713	Apple	macOS	Apple macOS Input Validation Error
CVE-2021-30657	Apple	macOS	Apple macOS Policy Subsystem Gatekeeper Bypass
CVE-2021-30665	Apple	Safari	Apple Safari Webkit Browser Engine Buffer Overflow Vulnerability
CVE-2021-30663	Apple	Safari	Apple Safari Webkit Browser Engine Integer Overflow Vulnerability

CVE-2021-30761	Apple	iOS	Apple WebKit Browser Engine Memory Corruption Vulnerability
CVE-2021-30869	Apple	iOS, macOS, and iPadOS	Apple XNU Kernel Type Confusion
CVE-2020-9859	Apple	iOS and iPadOS	Apple 11-13.5 XNU Kernel Vulnerability
CVE-2021-20090	Arcadyan	Buffalo WSR-2533DHPL2 and WSR-2533DHP3 firmware	Arcadyan Buffalo Firmware Multiple Versions Path Traversal
CVE-2021-27562	Arm	Arm Trusted Firmware	Arm Trusted Firmware M through 1.2 Denial-of-Service
CVE-2021-28664	Arm	Mali Graphics Processing Unit (GPU)	Arm Mali GPU Kernel Boundary Error Vulnerability
CVE-2021-28663	Arm	Mali Graphics Processing Unit (GPU)	Arm Mali GPU Kernel Use-After-Free Vulnerability
CVE-2019-3398	Atlassian	Confluence	Atlassian Confluence Path Traversal Vulnerability
CVE-2021-26084	Atlassian	Confluence Server	Atlassian Confluence Server < 6.13.23, 6.14.0 - 7.12.5 Arbitrary Code Execution
CVE-2019-11580	Atlassian	Crowd and Crowd Data Center	Atlassian Crowd and Crowd Data Center Remote Code Execution Vulnerability
CVE-2019-3396	Atlassian	Atlassian Confluence Server	Remote code execution via Widget Connector macro Vulnerability
CVE-2021-42258	BQE	BillQuick Web Suite	BQE BillQuick Web Suite Versions Prior to 22.0.9.1 (from 2018 through 2021) Remote Code Execution Vulnerability
CVE-2020-3452	Cisco	Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD)	Cisco Adaptive Security Appliance and Cisco Fire Power Threat Defense directory traversal sensitive file read
CVE-2020-3580	Cisco	Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD)	Cisco ASA and FTD XSS Vulnerabilities
CVE-2021-1497	Cisco	HyperFlex HX	Cisco HyperFlex HX Command Injection Vulnerabilities

CVE-2021-1498	Cisco	HyperFlex HX	Cisco HyperFlex HX Command Injection Vulnerabilities
CVE-2018-0171	Cisco	IOS and IOS XE	Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability
CVE-2020-3118	Cisco	IOS XR	Cisco IOS XR Software Cisco Discovery Protocol Format String Vulnerability
CVE-2020-3566	Cisco	IOS XR	Cisco IOS XR Software DVMRP Memory Exhaustion Vulnerability
CVE-2020-3569	Cisco	IOS XR	Cisco IOS XR Software DVMRP Memory Exhaustion Vulnerability
CVE-2020-3161	Cisco	IP Phones	Cisco IP Phones Web Server DoS and Remote Code Execution Vulnerability
CVE-2019-1653	Cisco	RV320 and RV325 Routers	Cisco RV320 and RV325 Routers Improper Access Control Vulnerability (COVID-19-CTI list)
CVE-2018-0296	Cisco	Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD)	Cisco Adaptive Security Appliance Firepower Threat Defense Denial-of-Service/Directory Traversal vulnerability
CVE-2019-13608	Citrix	StoreFront Server	Citrix StoreFront Server Multiple Versions XML External Entity (XXE)
CVE-2020-8193	Citrix	Application Delivery Controller (ADC), Gateway, and SDWAN WANOP	Citrix ADC, Citrix Gateway, Citrix SDWAN WANOP Unauthenticated Authorization Bypass
CVE-2020-8195	Citrix	Application Delivery Controller (ADC), Gateway, and SDWAN WANOP	Citrix ADC, Citrix Gateway, Citrix SDWAN WANOP Unauthenticated Authorization Bypass
CVE-2020-8196	Citrix	Application Delivery Controller (ADC), Gateway, and SDWAN WANOP	Citrix ADC, Citrix Gateway, Citrix SDWAN WANOP Unauthenticated Authorization Bypass
CVE-2019-19781	Citrix	Application Delivery Controller (ADC) and Gateway	Citrix Application Delivery Controller and Citrix Gateway Vulnerability
CVE-2019-11634	Citrix	Workspace (for Windows)	Citrix Workspace (for Windows) Prior to 1904 Improper Access Control
CVE-2020-29557	D-Link	DIR-825 R1	D-Link DIR-825 R1 Through 3.0.1 Before 11/2020 Buffer Overflow

CVE-2020-25506	D-Link	DNS-320	D-Link DNS-320 Command Injection Remote Code Execution Vulnerability
CVE-2018-15811	DNN	DotNetNuke (DNN)	DotNetNuke 9.2-9.2.2 Encryption Algorithm Vulnerability
CVE-2018-18325	DNN	DotNetNuke (DNN)	DotNetNuke 9.2-9.2.2 Encryption Algorithm Vulnerability
CVE-2017-9822	DNN	DotNetNuke (DNN)	DotNetNuke before 9.1.1 Remote Code Execution Vulnerability
CVE-2019-15752	Docker	Desktop Community Edition	Docker Desktop Community Edition Privilege Escalation Vulnerability
CVE-2020-8515	DrayTek	Vigor Router(s)	DrayTek Vigor Router Vulnerability
CVE-2018-7600	Drupal	Drupal	Drupal module configuration vulnerability
CVE-2021-22205	ExifTool	ExifTool	GitLab Community and Enterprise Editions From 11.9 Remote Code Execution Vulnerability
CVE-2018-6789	Exim	Exim	Exim Buffer Overflow Vulnerability
CVE-2020-8657	EyesOfNetwork	EyesOfNetwork	EyesOfNetwork 5.3 Insufficient Credential Protection
CVE-2020-8655	EyesOfNetwork	EyesOfNetwork	EyesOfNetwork 5.3 Privilege Escalation Vulnerability
CVE-2020-5902	F5	BIG-IP	F5 BIG-IP Traffic Management User Interface Remote Code Execution Vulnerability
CVE-2021-22986	F5	BIG-IP	F5 iControl REST unauthenticated Remote Code Execution Vulnerability
CVE-2021-35464	ForgeRock	Access Management server	ForgeRock Access Management Remote Code Execution Vulnerability
CVE-2019-5591	Fortinet	FortiOS	Fortinet FortiOS Default Configuration Vulnerability
CVE-2020-12812	Fortinet	FortiOS	Fortinet FortiOS SSL VPN 2FA Authentication Vulnerability
CVE-2018-13379	Fortinet	FortiOS	Fortinet FortiOS SSL VPN credential exposure vulnerability
CVE-2020-16010	Google	Chrome for Android	Google Chrome for Android Heap Overflow Vulnerability
CVE-2020-15999	Google	Chrome	Google Chrome FreeType Memory Corruption
CVE-2021-21166	Google	Chrome	Google Chrome Heap Buffer Overflow in WebAudio Vulnerability

CVE-2020-16017	Google	Chrome	Google Chrome Site Isolation Component Use-After-Free Remote Code Execution vulnerability
CVE-2021-37976	Google	Chrome	Google Chrome Information Leakage
CVE-2020-16009	Google	Chromium V8 Engine	Chromium V8 Implementation Vulnerability
CVE-2021-30632	Google	Chrome	Google Chrome Out-of-bounds write
CVE-2020-16013	Google	Chromium V8 Engine	Chromium V8 Incorrect Implementation Vulnerability
CVE-2021-30633	Google	Chrome	Google Chrome Use-After-Free Vulnerability
CVE-2021-21148	Google	Chromium V8 Engine	Chromium V8 JavaScript Rendering Engine Heap Buffer Overflow Vulnerability
CVE-2021-37973	Google	Chrome	Google Chrome Use-After-Free Vulnerability
CVE-2021-30551	Google	Chromium V8 Engine	Chromium V8 Type Confusion Vulnerability
CVE-2021-37975	Google	Chrome	Google Chrome Use-After-Free Vulnerability
CVE-2020-6418	Google	Chromium V8 Engine	Chromium V8 Type Confusion Vulnerability
CVE-2021-30554	Google	Chrome	Google Chrome WebGL Use-After-Free Vulnerability
CVE-2021-21206	Google	Chromium Blink	Chromium Blink Use-After-Free Vulnerability
CVE-2021-38000	Google	Chromium V8 Engine	Google Chromium V8 Insufficient Input Validation Vulnerability
CVE-2021-38003	Google	Chromium V8 Engine	Google Chromium V8 Incorrect Implementation Vulnerability
CVE-2021-21224	Google	Chromium V8 Engine	Chromium V8 JavaScript Engine Remote Code Execution Vulnerability
CVE-2021-21193	Google	Chromium V8 Engine	Chromium V8 Use-After-Free Vulnerability
CVE-2021-21220	Google	Chromium V8 Engine	Chromium V8 Input Validation Vulnerability
CVE-2021-30563	Google	Chrome	Google Chrome Browser V8 Arbitrary Code Execution
CVE-2020-4430	IBM	IBM Data Risk Manager	IBM Data Risk Manager Arbitrary File Download

CVE-2020-4427	IBM	IBM Data Risk Manager	IBM Data Risk Manager Authentication Bypass
CVE-2020-4428	IBM	IBM Data Risk Manager	IBM Data Risk Manager Command Injection
CVE-2019-4716	IBM	IBM Planning Analytics	IBM Planning Analytics configuration overwrite vulnerability
CVE-2016-3715	ImageMagick	ImageMagick	ImageMagick Ephemeral Coder Arbitrary File Deletion Vulnerability
CVE-2016-3718	ImageMagick	ImageMagick	ImageMagick SSRF Vulnerability
CVE-2020-15505	Ivanti	MobileIron Core & Connector	MobileIron Core, Connector, Sentry, and RDM Remote Code Execution Vulnerability
CVE-2021-30116	Kaseya	Kaseya VSA	Kaseya VSA Remote Code Execution Vulnerability
CVE-2020-7961	LifeRay	Liferay Portal	Liferay Portal prior to 7.2.1 CE GA2 Remote Code Execution Vulnerability
CVE-2021-23874	McAfee	McAfee Total Protection (MTP)	McAfee Total Protection MTP Arbitrary Process Execution
CVE-2021-22506	Micro Focus	Micro Focus Access Manager	Micro Focus Access Manager Earlier Than 5.0 Information Leakage
CVE-2021-22502	Micro Focus	Micro Focus Operation Bridge Reporter (OBR)	Micro Focus Operation Bridge Report (OBR) Server Remote Code Execution Vulnerability
CVE-2014-1812	Microsoft	Windows	Microsoft Windows Group Policy Privilege Escalation
CVE-2021-38647	Microsoft	Microsoft Azure Open Management Infrastructure (OMI)	Microsoft Azure Open Management Infrastructure (OMI) Remote Code Execution Vulnerability
CVE-2016-0167	Microsoft	Windows	Microsoft Windows Kernel 'Win32k.sys' Local Privilege Escalation Vulnerability
CVE-2020-0878	Microsoft	Microsoft Edge, Internet Explorer	Microsoft Browser Memory Corruption Vulnerability
CVE-2021-31955	Microsoft	Windows	Microsoft Windows Kernel Information Disclosure Vulnerability
CVE-2021-1647	Microsoft	Microsoft Defender	Microsoft Defender Remote Code Execution Vulnerability
CVE-2021-33739	Microsoft	Microsoft Desktop Window Manager (DWM)	Microsoft DWM Core Library Privilege Escalation Vulnerability

CVE-2016-0185	Microsoft	Windows	Microsoft Windows Media Center Remote Code Execution vulnerability
CVE-2020-0683	Microsoft	Windows	Microsoft Windows Installer Privilege Escalation Vulnerability
CVE-2020-17087	Microsoft	Windows	Microsoft Windows Kernel Cryptography Driver Privilege Escalation Vulnerability
CVE-2021-33742	Microsoft	Microsoft MSHTML	Microsoft MSHTML Platform Remote Code Execution Vulnerability
CVE-2021-31199	Microsoft	Microsoft Enhanced Cryptographic Provider	Microsoft Enhanced Cryptographic Provider Privilege Escalation Vulnerabilities
CVE-2021-33771	Microsoft	Windows	Microsoft Windows Kernel Privilege Escalation Vulnerability
CVE-2021-31956	Microsoft	Windows	Microsoft Windows NTFS Privilege Escalation Vulnerability
CVE-2021-31201	Microsoft	Microsoft Enhanced Cryptographic Provider	Microsoft Enhanced Cryptographic Provider Privilege Escalation Vulnerabilities
CVE-2021-31979	Microsoft	Windows	Microsoft Windows Kernel Privilege Escalation Vulnerability
CVE-2020-0938	Microsoft	Windows, Windows Adobe Type Manager Library	Microsoft Windows Type 1 Font Parsing Remote Code Execution Vulnerability
CVE-2020-17144	Microsoft	Microsoft Exchange Server	Microsoft Exchange Remote Code Execution Vulnerability
CVE-2020-0986	Microsoft	Windows	Microsoft Windows Kernel Privilege Escalation Vulnerability
CVE-2020-1020	Microsoft	Windows, Windows Adobe Type Manager Library	Microsoft Windows Type 1 Font Parsing Remote Code Execution Vulnerability
CVE-2021-38645	Microsoft	Microsoft Azure Open Management Infrastructure (OMI)	Microsoft Azure Open Management Infrastructure (OMI) Privilege Escalation Vulnerability
CVE-2021-34523	Microsoft	Microsoft Exchange Server	Microsoft Exchange Server Privilege Escalation Vulnerability
CVE-2017-7269	Microsoft	Internet Information Services (IIS)	Microsoft Windows Server 2003 R2 IIS WEBDAV buffer overflow Remote Code Execution vulnerability (COVID-19-CTI list)
CVE-2021-36948	Microsoft	Windows	Microsoft Windows Update Medic Service Privilege Escalation

			Vulnerability
CVE-2021-38649	Microsoft	Microsoft Azure Open Management Infrastructure (OMI)	Microsoft Azure Open Management Infrastructure (OMI) Privilege Escalation Vulnerability
CVE-2020-0688	Microsoft	Microsoft Exchange Server	Microsoft Exchange Server Key Validation Vulnerability
CVE-2017-0143	Microsoft	SMBv1 server	Microsoft Windows SMBv1 Remote Code Execution Vulnerability
CVE-2016-7255	Microsoft	Windows	Microsoft Windows Vista, 7, 8.1, 10 and Windows Server 2008, 2012, and 2016 Win32k Privilege Escalation Vulnerability
CVE-2019-0708	Microsoft	Remote Desktop Services	"BlueKeep" Microsoft Windows Remote Desktop Remote Code Execution Vulnerability
CVE-2021-34473	Microsoft	Microsoft Exchange Server	Microsoft Exchange Server Remote Code Execution Vulnerability
CVE-2020-1464	Microsoft	Windows	Microsoft Windows Spoofing Vulnerability
CVE-2021-1732	Microsoft	Win32k	Microsoft Win32k Privilege Escalation Vulnerability
CVE-2021-34527	Microsoft	Windows	"PrintNightmare" - Microsoft Windows Print Spooler Remote Code Execution Vulnerability
CVE-2021-31207	Microsoft	Microsoft Exchange Server	Microsoft Exchange Server Security Feature Bypass Vulnerability
CVE-2019-0803	Microsoft	Win32k	Microsoft Win32k Escalation Kernel Vulnerability
CVE-2020-1040	Microsoft	Hyper-V RemoteFX vGPU	Hyper-V RemoteFX vGPU Remote Code Execution Vulnerability
CVE-2021-28310	Microsoft	Win32k	Microsoft Win32k Privilege Escalation Vulnerability
CVE-2020-1350	Microsoft	Windows	"SigRed" - Microsoft Windows Domain Name System (DNS) Server Remote Code Execution Vulnerability
CVE-2021-26411	Microsoft	Microsoft Edge, Internet Explorer	Microsoft Internet Explorer and Edge Memory Corruption Vulnerability
CVE-2019-0859	Microsoft	Win32k	Microsoft Win32k Escalation Kernel Vulnerability
CVE-2021-40444	Microsoft	Microsoft MSHTML	Microsoft Windows, Server (spec. IE) All Arbitrary Code Execution

CVE-2017-8759	Microsoft	Microsoft .NET Framework	.NET Framework Remote Code Execution vulnerability
CVE-2018-8653	Microsoft	Internet Explorer Scripting Engine	Microsoft Internet Explorer Scripting Engine JScript Memory Corruption Vulnerability
CVE-2019-0797	Microsoft	Win32k	Microsoft Win32k.sys Driver Vulnerability
CVE-2021-36942	Microsoft	Windows	Microsoft Windows Local Security Authority (LSA) Spoofing
CVE-2019-1215	Microsoft	Windows	Microsoft Windows Winsock (ws2ifsl.sys) Vulnerability
CVE-2018-0798	Microsoft	Office	Microsoft Office 2007 - 2016 Backdoor Exploitation Chain
CVE-2018-0802	Microsoft	Office	Microsoft Office 2007 - 2016 Backdoor Exploitation Chain
CVE-2012-0158	Microsoft	MSCOMCTL.OCX	Microsoft MSCOMCTL.OCX Remote Code Execution Vulnerability
CVE-2015-1641	Microsoft	Office	Microsoft Office Memory Corruption vulnerability
CVE-2021-27085	Microsoft	Internet Explorer	Internet Explorer 11 Remote Code Execution Vulnerability
CVE-2019-0541	Microsoft	MSHTML engine	Microsoft MSHTML Engine Remote Code Execution Vulnerability
CVE-2017-11882	Microsoft	Office	Microsoft Office memory corruption vulnerability
CVE-2020-0674	Microsoft	Internet Explorer Scripting Engine	Internet Explorer 9-11 Scripting Engine Memory Corruption Vulnerability
CVE-2021-27059	Microsoft	Office	Microsoft Office Remote Code Execution Vulnerability
CVE-2019-1367	Microsoft	Internet Explorer Scripting Engine	Internet Explorer 9-11 Scripting Engine Memory Corruption Vulnerability
CVE-2017-0199	Microsoft	Windows, Windows Server, Office	Microsoft Office/WordPad Remote Code Execution Vulnerability with Windows API
CVE-2020-1380	Microsoft	Internet Explorer	Scripting Engine Memory Corruption Vulnerability
CVE-2019-1429	Microsoft	Internet Explorer Scripting Engine	Internet Explorer 9-11 Scripting Engine Memory Corruption Vulnerability
CVE-2017-11774	Microsoft	Microsoft Outlook	Microsoft Outlook Security Feature Bypass Vulnerability

CVE-2020-0968	Microsoft	Internet Explorer Scripting Engine	Internet Explorer Scripting Engine Memory Corruption Vulnerability
CVE-2020-1472	Microsoft	Netlogon Remote Protocol (MS-NRPC)	NetLogon Privilege Escalation Vulnerability
CVE-2021-26855	Microsoft	Microsoft Exchange Server	Microsoft OWA Exchange Control Panel (ECP) Exploit Chain
CVE-2021-26858	Microsoft	Microsoft Exchange Server	Microsoft OWA Exchange Control Panel (ECP) Exploit Chain
CVE-2021-27065	Microsoft	Microsoft Exchange Server	Microsoft OWA Exchange Control Panel (ECP) Exploit Chain
CVE-2020-1054	Microsoft	Win32k	Microsoft Win32k Privilege Escalation Vulnerability
CVE-2021-1675	Microsoft	Windows	Microsoft Windows Print Spooler Remote Code Execution Vulnerability
CVE-2021-34448	Microsoft	Scripting Engine	Microsoft Scripting Engine Memory Corruption Vulnerability
CVE-2020-0601	Microsoft	Windows CryptoAPI	Microsoft Windows 10 API/ECC Vulnerability
CVE-2019-0604	Microsoft	SharePoint	Microsoft SharePoint Remote Code Execution Vulnerability
CVE-2020-0646	Microsoft	Microsoft .NET Framework	Microsoft .NET Framework Remote Code Execution Vulnerability
CVE-2019-0808	Microsoft	Windows	Microsoft Windows 7 win32k.sys Driver Vulnerability
CVE-2021-26857	Microsoft	Microsoft Exchange Server	Microsoft Unified Messaging Deserialization Vulnerability
CVE-2020-1147	Microsoft	Microsoft .NET Framework, Microsoft SharePoint, Visual Studio	Microsoft .NET Framework, SharePoint Server, and Visual Studio Remote Code Execution Vulnerability
CVE-2019-1214	Microsoft	Windows	Microsoft Windows Common Log File System (CLFS) Driver Vulnerability
CVE-2016-3235	Microsoft	Microsoft Visio/Office	Microsoft Visio/Office OLE DLL Side Loading vulnerability
CVE-2019-0863	Microsoft	Windows	Microsoft Windows Error Reporting (WER) Vulnerability
CVE-2021-36955	Microsoft	Windows	Microsoft Windows Common Log File System (CLFS) Driver Privilege Escalation Vulnerability
CVE-2021-38648	Microsoft	Microsoft Azure Open Management Infrastructure (OMI)	Microsoft Azure Open Management Infrastructure (OMI) Privilege Escalation Vulnerability

CVE-2020-6819	Mozilla	nsDocShell destructor	Mozilla Firefox 74 and Firefox ESR 68.6 nsDocShell vulnerability
CVE-2020-6820	Mozilla	ReadableStream	Mozilla Firefox 74 and Firefox ESR 68.6 ReadableStream vulnerability
CVE-2019-17026	Mozilla	IonMonkey JIT compiler	Mozilla Firefox IonMonkey JIT compiler Type Confusion Vulnerability
CVE-2019-15949	Nagios	Nagios XI	Nagios XI Remote Code Execution Vulnerability
CVE-2020-26919	Netgear	NETGEAR JGS516PE devices	Netgear ProSAFE Plus JGS516PE Remote Code Execution vulnerability
CVE-2019-19356	Netis	Netis WF2419	Netis WF2419 Router Tracert Remote Code Execution vulnerability
CVE-2020-2555	Oracle	Oracle Coherence	Oracle Coherence Deserialization Remote Code Execution
CVE-2012-3152	Oracle	Oracle Reports Developer	Oracle Reports Developer Arbitrary File Read and Upload vulnerability
CVE-2020-14871	Oracle	Oracle Solaris	Oracle Solaris Pluggable Authentication Module vulnerability
CVE-2015-4852	Oracle	Oracle WebLogic Server	Oracle WebLogic Server Remote Code Execution Vulnerability
CVE-2020-14750	Oracle	Oracle WebLogic Server	Oracle WebLogic Server Remote Code Execution Vulnerability
CVE-2020-14882	Oracle	Oracle WebLogic Server	Oracle WebLogic Server Remote Code Execution Vulnerability
CVE-2020-14883	Oracle	Oracle WebLogic Server	Oracle WebLogic Server Remote Code Execution Vulnerability
CVE-2020-8644	PlaySMS	PlaySMS	PlaySMS Remote Code Execution Vulnerability
CVE-2019-18935	Progress	ASP.NET AJAX	Progress Telerik UI for ASP.NET deserialization bug
CVE-2021-22893	Pulse Secure	Pulse Connect Secure	Pulse Connect Secure Remote Code Execution Vulnerability
CVE-2020-8243	Pulse Secure	Pulse Connect Secure	Pulse Connect Secure Arbitrary Code Execution
CVE-2021-22900	Pulse Secure	Pulse Connect Secure	Pulse Connect Secure Arbitrary File Upload Vulnerability
CVE-2021-22894	Pulse Secure	Pulse Connect Secure	Pulse Connect Secure Collaboration Suite Remote Code Execution Vulnerability
CVE-2020-8260	Pulse Secure	Pulse Connect Secure	Pulse Connect Secure Remote Code Execution Vulnerability

CVE-2021-22899	Pulse Secure	Pulse Connect Secure	Pulse Connect Secure Remote Code Execution Vulnerability
CVE-2019-11510	Pulse Secure	Pulse Connect Secure	Pulse Connect Secure VPN arbitrary file reading vulnerability (COVID-19-CTI list)
CVE-2019-11539	Pulse Secure	Pulse Connect Secure, Policy Secure	Pulse Connect Secure and Policy Secure Multiple Versions Code Execution
CVE-2021-1906	Qualcomm	Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	Qualcomm Improper Error Handling Vulnerability
CVE-2021-1905	Qualcomm	Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	Qualcomm Use-After-Free Vulnerability
CVE-2020-10221	rConfig	rConfig	rConfig Remote Code Execution Vulnerability
CVE-2021-35395	Realtek	Jungle Software Development Kit (SDK)	Realtek SDK Arbitrary Code Execution
CVE-2017-16651	Roundcube	Roundcube Webmail	Roundcube Webmail File Disclosure Vulnerability
CVE-2020-11652	SaltStack	Salt	SaltStack directory traversal failure to sanitize untrusted input
CVE-2020-11651	SaltStack	Salt	SaltStack Salt Authentication Bypass
CVE-2020-16846	SaltStack	Salt	SaltStack Through 3002 Shell Injection Vulnerability
CVE-2018-2380	SAP	SAP CRM	SAP NetWeaver AS JAVA CRM Remote Code Execution Vulnerability

CVE-2010-5326	SAP	SAP NetWeaver Application Server Java platforms	SAP NetWeaver AS JAVA Remote Code Execution Vulnerability
CVE-2016-9563	SAP	SAP NetWeaver AS JAVA	SAP NetWeaver AS JAVA XXE Vulnerability
CVE-2020-6287	SAP	SAP NetWeaver AS JAVA (LM Configuration Wizard)	SAP Netweaver JAVA remote unauthenticated access vulnerability
CVE-2020-6207	SAP	SAP Solution Manager (User Experience Monitoring)	SAP Solution Manager Missing Authentication Check Complete Compromise of SMD Agents vulnerability
CVE-2016-3976	SAP	SAP NetWeaver AS Java	SAP NetWeaver AS Java 7.1 - 7.5 Directory Traversal Vulnerability
CVE-2019-16256	SIMalliance	SIMalliance Toolbox (S@T) Browser	SIMalliance Toolbox (S@T) Browser Command and Control Vulnerability
CVE-2020-10148	SolarWinds	SolarWinds Orion Platform	SolarWinds Orion API Authentication Bypass Vulnerability
CVE-2021-35211	SolarWinds	SolarWinds nServ-U	SolarWinds Serv-U Remote Memory Escape Vulnerability
CVE-2016-3643	SolarWinds	SolarWinds Virtualization Manager	SolarWinds Virtualization Manager Privilege Escalation Vulnerability
CVE-2020-10199	Sonatype	Sonatype Nexus Repository	Nexus Repository Manager 3 Remote Code Execution Vulnerability
CVE-2021-20021	SonicWall	SonicWall Email Security	SonicWall Email Security Privilege Escalation Exploit Chain
CVE-2019-7481	SonicWall	SMA100	SonicWall SMA100 9.0.0.3 and Earlier SQL Injection
CVE-2021-20022	SonicWall	SonicWall Email Security	SonicWall Email Security Privilege Escalation Exploit Chain
CVE-2021-20023	SonicWall	SonicWall Email Security	SonicWall Email Security Privilege Escalation Exploit Chain
CVE-2021-20016	SonicWall	SonicWall SSLVPN SMA100	SonicWall SSL VPN SMA100 SQL Injection Vulnerability
CVE-2020-12271	Sophos	Sophos XG Firewall devices	Sophos XG Firewall SQL Injection Vulnerability
CVE-2020-10181	Sumavision	Sumavision Enhanced Multimedia Router EMR	Sumavision EMR 3.0 CSRF Vulnerability
CVE-2017-6327	Symantec	Symantec Messaging Gateway	Symantec Messaging Gateway Remote Code Execution Vulnerability

CVE-2019-18988	TeamViewer	TeamViewer Desktop	TeamViewer Desktop Bypass Remote Login
CVE-2017-9248	Telerik	ASP.NET AJAX and Sitefinity	Telerik UI for ASP.NET AJAX and Progress Sitefinity Cryptographic Weakness Vuln
CVE-2021-31755	Tenda	Tenda AC11 devices	Tenda AC11 Up to 02.03.01.104_CN Stack Buffer Overflow
CVE-2020-10987	Tenda	Tenda AC15 AC1900	Tenda Router Code Execution
CVE-2018-14558	Tenda	Tenda AC7, AC9, and AC10 devices	Tenda Router Command Injection Vulnerability
CVE-2018-20062	ThinkPHP	NoneCms	ThinkPHP Remote Code Execution Vulnerability
CVE-2019-9082	ThinkPHP	ThinkPHP	ThinkPHP Remote Code Execution Vulnerability
CVE-2019-18187	Trend Micro	Trend Micro OfficeScan	Trend Micro Antivirus Oday Traversal Vulnerability
CVE-2020-8467	Trend Micro	Trend Micro Apex One and OfficeScan XG	Trend Micro Apex One (2019) and OfficeScan XG migration tool remote code execution vulnerability
CVE-2020-8468	Trend Micro	Trend Micro Apex One, OfficeScan XG and Worry-Free Business Security	Trend Micro Apex One (2019), OfficeScan XG and Worry-Free Business Security (9.0, 9.5, 10.0) agent content validation escape vulnerability
CVE-2020-24557	Trend Micro	Trend Micro Apex One and Worry-Free Business Security	Trend Micro Apex One and OfficeScan XG Improper Access Control Privilege Escalation Vulnerability
CVE-2020-8599	Trend Micro	Trend Micro Apex One and OfficeScan XG server	Trend Micro Apex One and OfficeScan XG Vulnerability
CVE-2021-36742	Trend Micro	Trend Micro Multiple Products	Trend Micro Systems Multiple Products Buffer Overflow - Arbitrary File Upload
CVE-2021-36741	Trend Micro	Trend Micro Multiple Products	Trend Micro Systems Multiple Products Buffer Overflow - Arbitrary File Upload
CVE-2019-20085	TVT	NVMS-1000	TVT NVMS-1000 Directory Traversal
CVE-2020-5849	Unraid	Unraid	Unraid 6.8.0 Authentication Bypass
CVE-2020-5847	Unraid	Unraid	Unraid 6.8.0 Remote Code Execution Vulnerability

CVE-2019-16759	vBulletin	vBulletin	vBulletin PHP Module Remote Code Execution Vulnerability
CVE-2020-17496	vBulletin	vBulletin	vBulletin PHP Module Remote Code Execution Vulnerability
CVE-2019-5544	VMware	ESXi, Horizon DaaS Appliances	VMware ESXi/Horizon DaaS Appliances Heap-Overwrite Vulnerability
CVE-2020-3992	VMware	ESXi	OpenSLP as used in VMware ESXi
CVE-2020-3950	VMware	VMware Fusion, VMware Remote Console for Mac, and Horizon Client for Mac	VMware Privilege escalation vulnerability
CVE-2021-22005	VMware	vCenter Server	VMware vCenter Server File Upload
CVE-2020-3952	VMware	vCenter Server	VMware vCenter Server Info Disclosure Vulnerability
CVE-2021-21972	VMware	vCenter Server	VMware vCenter Server Remote Code Execution Vulnerability
CVE-2021-21985	VMware	vCenter Server	VMware vCenter Server Remote Code Execution Vulnerability
CVE-2020-4006	VMware	VMware Workspace One Access, Access Connector, Identity Manager, and Identity Manager Connector	VMware Workspace One Access, Access Connector, Identity Manager, and Identity Manager Connector Command Injection vulnerability
CVE-2020-25213	WordPress	File Manager	WordPress File Manager Remote Code Execution Vulnerability
CVE-2020-11738	WordPress	Snap Creek Duplicator	WordPress Snap Creek Duplicator and Duplicator Pro plugins Directory Traversal
CVE-2019-9978	WordPress	Social-Warfare	WordPress Social-Warfare plugin XSS
CVE-2021-27561	Yealink	Device Management Platform	Yealink Device Management Server Pre-Authorization SSRF
CVE-2021-40539	Zoho	ManageEngine ADSelfServicePlus	Zoho Corp. ManageEngine ADSelfService Plus Version 6113 and Earlier Authentication Bypass
CVE-2020-10189	Zoho	ManageEngine Desktop Central	Zoho ManageEngine Desktop Central Remote Code Execution Vulnerability
CVE-2019-8394	Zoho	ManageEngine ServiceDesk Plus (SDP)	Zoho ManageEngine ServiceDesk Plus Arbitrary File Upload Vulnerability
CVE-2020-29583	ZyXEL	Unified Security Gateway (USG)	ZyXEL Unified Security Gateway Undocumented Administrator Account with Default Credentials

CVE-2021-22204	Perl	Exiftool	ExifTool Remote Code Execution Vulnerability
CVE-2021-40449	Microsoft	Windows	Microsoft Windows Win32k Privilege Escalation Vulnerability
CVE-2021-42321	Microsoft	Exchange	Microsoft Exchange Server Remote Code Execution Vulnerability
CVE-2021-42292	Microsoft	Office	Microsoft Excel Security Feature Bypass
CVE-2020-11261	Qualcomm	Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	Qualcomm Multiple Chipsets Improper Input Validation Vulnerability
CVE-2018-14847	MikroTik	RouterOS	MikroTik Router OS Directory Traversal Vulnerability
CVE-2021-37415	Zoho	ManageEngine ServiceDesk Plus (SDP)	Zoho ManageEngine ServiceDesk Authentication Bypass Vulnerability
CVE-2021-40438	Apache	Apache	Apache HTTP Server-Side Request Forgery (SSRF)
CVE-2021-44077	Zoho	ManageEngine ServiceDesk Plus (SDP) / SupportCenter Plus	Zoho ManageEngine ServiceDesk Plus Remote Code Execution Vulnerability
CVE-2021-44515	Zoho	Desktop Central	Zoho Desktop Central Authentication Bypass Vulnerability
CVE-2019-13272	Linux	Kernel	Linux Kernel Improper Privilege Management Vulnerability
CVE-2021-35394	Realtek	Jungle Software Development Kit (SDK)	Realtek Jungle SDK Remote Code Execution Vulnerability
CVE-2019-7238	Sonatype	Nexus Repository Manager	Sonatype Nexus Repository Manager Incorrect Access Control Vulnerability
CVE-2019-0193	Apache	Solr	Apache Solr DataImportHandler Code Injection Vulnerability
CVE-2021-44168	Fortinet	FortiOS	Fortinet FortiOS Arbitrary File Download
CVE-2017-17562	Embedthis	GoAhead	Embedthis GoAhead Remote Code Execution Vulnerability

CVE-2017-12149	Red Hat	JBoss Application Server	Red Hat JBoss Application Server Remote Code Execution Vulnerability
CVE-2010-1871	Red Hat	JBoss Seam 2	Red Hat Linux JBoss Seam 2 Remote Code Execution Vulnerability
CVE-2020-17463	Fuel CMS		Fuel CMS SQL Injection Vulnerability
CVE-2020-8816	Pi-hole	AdminLTE	Pi-Hole AdminLTE Remote Code Execution Vulnerability
CVE-2019-10758	MongoDB	mongo-express	MongoDB mongo-express Remote Code Execution Vulnerability
CVE-2021-44228	Apache	Log4j2	Apache Log4j2 Remote Code Execution Vulnerability
CVE-2021-43890	Microsoft	Windows	Microsoft Windows AppX Installer Spoofing Vulnerability
CVE-2021-4102	Google	Chromium V8 Engine	Google Chromium V8 Use-After-Free Vulnerability
CVE-2021-22017	VMware	vCenter Server	VMware vCenter Server Improper Access Control
CVE-2021-36260	Hikvision	Security cameras web server	Hikvision Improper Input Validation
CVE-2020-6572	Google	Chrome	Google Chrome Prior to 81.0.4044.92 Use-After-Free Vulnerability
CVE-2019-1458	Microsoft	Win32k	Microsoft Win32k Privilege Escalation Vulnerability
CVE-2013-3900	Microsoft	WinVerifyTrust function	Microsoft WinVerifyTrust function Remote Code Execution
CVE-2019-2725	Oracle	WebLogic Server	Oracle WebLogic Server, Injection
CVE-2019-9670	Synacor	Zimbra Collaboration Suite	Synacor Zimbra Collaboration Suite Improper Restriction of XML External Entity Reference
CVE-2018-13382	Fortinet	FortiOS and FortiProxy	Fortinet FortiOS and FortiProxy Improper Authorization
CVE-2018-13383	Fortinet	FortiOS and FortiProxy	Fortinet FortiOS and FortiProxy Out-of-bounds Write
CVE-2019-1579	Palo Alto Networks	PAN-OS	Palo Alto Networks PAN-OS Remote Code Execution Vulnerability
CVE-2019-10149	Exim	Mail Transfer Agent (MTA)	Exim Mail Transfer Agent (MTA) Improper Input Validation
CVE-2015-7450	IBM	WebSphere Application Server and Server Hypervisor Edition	IBM WebSphere Application Server and Server Hypervisor Edition Code Injection.

CVE-2017-1000486	Primetek	Primefaces Application	Primetek Primefaces Remote Code Execution Vulnerability
CVE-2019-7609	Elastic	Kibana	Kibana Arbitrary Code Execution
CVE-2021-27860	FatPipe	WARP, IPVPN, and MPVPN software	FatPipe WARP, IPVPN, and MPVPN Configuration Upload exploit
CVE-2021-32648	October CMS	October CMS	October CMS Improper Authentication
CVE-2021-25296	Nagios	Nagios XI	Nagios XI OS Command Injection
CVE-2021-25297	Nagios	Nagios XI	Nagios XI OS Command Injection
CVE-2021-25298	Nagios	Nagios XI	Nagios XI OS Command Injection
CVE-2021-40870	Aviatrix	Aviatrix Controller	Aviatrix Controller Unrestricted Upload of File
CVE-2021-33766	Microsoft	Exchange Server	Microsoft Exchange Server Information Disclosure
CVE-2021-21975	VMware	vRealize Operations Manager API	VMware Server Side Request Forgery in vRealize Operations Manager API
CVE-2021-21315	Npm package	System Information Library for Node.JS	System Information Library for Node.JS Command Injection
CVE-2021-22991	F5	BIG-IP Traffic Management Microkernel	F5 BIG-IP Traffic Management Microkernel Buffer Overflow
CVE-2020-14864	Oracle	Intelligence Enterprise Edition	Oracle Business Intelligence Enterprise Edition Path Transversal
CVE-2020-13671	Drupal	Drupal core	Drupal core Un-restricted Upload of File
CVE-2020-11978	Apache	Airflow	Apache Airflow Command Injection
CVE-2020-13927	Apache	Airflow's Experimental API	Apache Airflow's Experimental API Authentication Bypass
CVE-2006-1547	Apache	Struts 1	Apache Struts 1 ActionForm Denial-of-Service Vulnerability
CVE-2012-0391	Apache	Struts 2	Apache Struts 2 Improper Input Validation Vulnerability
CVE-2018-8453	Microsoft	Win32k	Microsoft Win32k Privilege Escalation Vulnerability
CVE-2021-35247	SolarWinds	Serv-U	SolarWinds Serv-U Improper Input Validation Vulnerability
CVE-2022-22587	Apple	iOS and macOS	Apple Memory Corruption Vulnerability
CVE-2021-20038	SonicWall	SMA 100 Appliances	SonicWall SMA 100 Appliances Stack-Based Buffer Overflow Vulnerability

CVE-2020-5722	Grandstream	UCM6200	Grandstream Networks UCM6200 Series SQL Injection Vulnerability
CVE-2020-0787	Microsoft	Windows	Microsoft Windows Background Intelligent Transfer Service (BITS) Improper Privilege Management Vulnerability
CVE-2017-5689	Intel	Active Management Technology (AMT), Small Business Technology (SBT), and Standard Manageability	Intel Active Management Technology (AMT), Small Business Technology (SBT), and Standard Manageability Privilege Escalation Vulnerability
CVE-2014-1776	Microsoft	Internet Explorer	Microsoft Internet Explorer Use-After-Free Vulnerability
CVE-2014-6271	GNU	Bourne-Again Shell (Bash)	GNU Bourne-Again Shell (Bash) Arbitrary Code Execution Vulnerability
CVE-2014-7169	GNU	Bourne-Again Shell (Bash)	GNU Bourne-Again Shell (Bash) Arbitrary Code Execution Vulnerability
CVE-2022-21882	Microsoft	Win32k	Microsoft Win32k Privilege Escalation Vulnerability
CVE-2021-36934	Microsoft	Windows	Microsoft Windows SAM Local Privilege Escalation Vulnerability
CVE-2020-0796	Microsoft	SMBv3	Microsoft SMBv3 Remote Code Execution Vulnerability
CVE-2018-1000861	Jenkins	Jenkins Stapler Web Framework	Jenkins Stapler Web Framework Deserialization of Untrusted Data Vulnerability
CVE-2017-9791	Apache	Struts 1	Apache Struts 1 Improper Input Validation Vulnerability
CVE-2017-8464	Microsoft	Windows	Microsoft Windows Shell (.lnk) Remote Code Execution Vulnerability
CVE-2017-10271	Oracle	WebLogic Server	Oracle Corporation WebLogic Server Remote Code Execution Vulnerability
CVE-2017-0263	Microsoft	Win32k	Microsoft Win32k Privilege Escalation Vulnerability
CVE-2017-0262	Microsoft	Office	Microsoft Office Remote Code Execution Vulnerability
CVE-2017-0145	Microsoft	SMBv1	Microsoft SMBv1 Remote Code Execution Vulnerability
CVE-2017-0144	Microsoft	SMBv1	Microsoft SMBv1 Remote Code Execution Vulnerability
CVE-2016-3088	Apache	ActiveMQ	Apache ActiveMQ Improper Input Validation Vulnerability

CVE-2015-2051	D-Link	DIR-645 Router	D-Link DIR-645 Router Remote Code Execution Vulnerability
CVE-2015-1635	Microsoft	HTTP.sys	Microsoft HTTP.sys Remote Code Execution Vulnerability
CVE-2015-1130	Apple	OS X	Apple OS X Authentication Bypass Vulnerability
CVE-2014-4404	Apple	OS X	Apple OS X Heap-Based Buffer Overflow Vulnerability
CVE-2022-22620	Apple	Webkit	Apple Webkit Remote Code Execution Vulnerability
CVE-2022-24086	Adobe	Commerce and Magento Open Source	Adobe Commerce and Magento Open Source Improper Input Validation Vulnerability
CVE-2022-0609	Google	Chrome	Google Chrome Use-After-Free Vulnerability
CVE-2019-0752	Microsoft	Internet Explorer	Microsoft Internet Explorer Type Confusion Vulnerability
CVE-2018-8174	Microsoft	Windows	Microsoft Windows VBScript Engine Out-of-Bounds Write Vulnerability
CVE-2018-20250	RARLAB	WinRAR	WinRAR Absolute Path Traversal Vulnerability
CVE-2018-15982	Adobe	Flash Player	Adobe Flash Player Use-After-Free Vulnerability
CVE-2017-9841	PHPUnit	PHPUnit	PHPUnit Command Injection Vulnerability
CVE-2014-1761	Microsoft	Word	Microsoft Word Memory Corruption Vulnerability
CVE-2013-3906	Microsoft	Graphics Component	Microsoft Graphics Component Memory Corruption Vulnerability
CVE-2022-23131	Zabbix	Frontend	Zabbix Frontend Authentication Bypass Vulnerability
CVE-2022-23134	Zabbix	Frontend	Zabbix Frontend Improper Access Control Vulnerability
CVE-2022-24682	Zimbra	Webmail	Zimbra Webmail Cross-Site Scripting Vulnerability
CVE-2017-8570	Microsoft	Office	Microsoft Office Remote Code Execution Vulnerability
CVE-2017-0222	Microsoft	Internet Explorer	Microsoft Internet Explorer Remote Code Execution Vulnerability
CVE-2014-6352	Microsoft	Windows	Microsoft Windows Code Injection Vulnerability

CVE-2022-20708	Cisco	Small Business RV160, RV260, RV340, and RV345 Series Routers	Cisco Small Business RV Series Routers Stack-based Buffer Overflow Vulnerability
CVE-2022-20703	Cisco	Small Business RV160, RV260, RV340, and RV345 Series Routers	Cisco Small Business RV Series Routers Stack-based Buffer Overflow Vulnerability
CVE-2022-20701	Cisco	Small Business RV160, RV260, RV340, and RV345 Series Routers	Cisco Small Business RV Series Routers Stack-based Buffer Overflow Vulnerability
CVE-2022-20700	Cisco	Small Business RV160, RV260, RV340, and RV345 Series Routers	Cisco Small Business RV Series Routers Stack-based Buffer Overflow Vulnerability
CVE-2022-20699	Cisco	Small Business RV160, RV260, RV340, and RV345 Series Routers	Cisco Small Business RV Series Routers Stack-based Buffer Overflow Vulnerability
CVE-2021-41379	Microsoft	Windows	Microsoft Windows Installer Privilege Escalation Vulnerability
CVE-2020-1938	Apache	Tomcat	Apache Tomcat Improper Privilege Management Vulnerability
CVE-2020-11899	Treck TCP/IP stack	IPv6	Treck TCP/IP stack Out-of-Bounds Read Vulnerability
CVE-2019-16928	Exim	Exim Internet Mailer	Exim Out-of-bounds Write Vulnerability
CVE-2019-1652	Cisco	Small Business RV320 and RV325 Dual Gigabit WAN VPN Routers	Cisco Small Business Routers Improper Input Validation Vulnerability
CVE-2019-1297	Microsoft	Excel	Microsoft Excel Remote Code Execution Vulnerability
CVE-2018-8581	Microsoft	Exchange Server	Microsoft Exchange Server Privilege Escalation Vulnerability
CVE-2018-8298	ChakraCore	ChakraCore scripting engine	ChakraCore Scripting Engine Type Confusion Vulnerability
CVE-2018-0180	Cisco	IOS Software	Cisco IOS Software Denial-of-Service Vulnerability
CVE-2018-0179	Cisco	IOS Software	Cisco IOS Software Denial-of-Service Vulnerability
CVE-2018-0175	Cisco	IOS, XR, and XE Software	Cisco IOS, XR, and XE Software Buffer Overflow Vulnerability
CVE-2018-0174	Cisco	IOS XE Software	Cisco IOS Software and Cisco IOS XE Software Improper Input Validation Vulnerability

CVE-2018-0173	Cisco	IOS and IOS XE Software	Cisco IOS and IOS XE Software Improper Input Validation Vulnerability
CVE-2018-0172	Cisco	IOS and IOS XE Software	Cisco IOS and IOS XE Software Improper Input Validation Vulnerability
CVE-2018-0167	Cisco	IOS, XR, and XE Software	Cisco IOS, XR, and XE Software Buffer Overflow Vulnerability
CVE-2018-0161	Cisco	IOS Software	Cisco IOS Software Resource Management Errors Vulnerability
CVE-2018-0159	Cisco	IOS Software and Cisco IOS XE Software	Cisco IOS and XE Software Internet Key Exchange Version 1 Denial-of-Service Vulnerability
CVE-2018-0158	Cisco	IOS Software and Cisco IOS XE Software	Cisco IOS and XE Software Internet Key Exchange Memory Leak Vulnerability
CVE-2018-0156	Cisco	IOS Software and Cisco IOS XE Software	Cisco IOS Software and Cisco IOS XE Software Smart Install Denial-of-Service Vulnerability
CVE-2018-0155	Cisco	Catalyst 4500 Series Switches and Cisco Catalyst 4500-X Series Switches	Cisco Catalyst Bidirectional Forwarding Detection Denial-of-Service Vulnerability
CVE-2018-0154	Cisco	IOS Software	Cisco IOS Software Integrated Services Module for VPN Denial-of-Service Vulnerability
CVE-2018-0151	Cisco	IOS and IOS XE Software	Cisco IOS Software and Cisco IOS XE Software Quality of Service Remote Code Execution Vulnerability
CVE-2017-8540	Microsoft	Malware Protection Engine	Microsoft Malware Protection Engine Improper Restriction of Operations Vulnerability
CVE-2017-6744	Cisco	IOS software	Cisco IOS Software SNMP Remote Code Execution Vulnerability
CVE-2017-6743	Cisco	IOS and IOS XE Software	Cisco IOS and IOS XE Software SNMP Remote Code Execution Vulnerability
CVE-2017-6740	Cisco	IOS and IOS XE Software	Cisco IOS and IOS XE Software SNMP Remote Code Execution Vulnerability
CVE-2017-6739	Cisco	IOS and IOS XE Software	Cisco IOS and IOS XE Software SNMP Remote Code Execution Vulnerability
CVE-2017-6738	Cisco	IOS and IOS XE Software	Cisco IOS and IOS XE Software SNMP Remote Code Execution Vulnerability

CVE-2017-6737	Cisco	IOS and IOS XE Software	Cisco IOS and IOS XE Software SNMP Remote Code Execution Vulnerability
CVE-2017-6736	Cisco	IOS and IOS XE Software	Cisco IOS and IOS XE Software SNMP Remote Code Execution Vulnerability
CVE-2017-6663	Cisco	IOS and IOS XE Software	Cisco IOS Software and Cisco IOS XE Software Denial-of-Service Vulnerability
CVE-2017-6627	Cisco	IOS and IOS XE Software	Cisco IOS Software and Cisco IOS XE Software UDP Packet Processing Denial-of-Service Vulnerability
CVE-2017-12319	Cisco	IOS XE Software	Cisco IOS XE Software Ethernet Virtual Private Network Border Gateway Protocol Denial-of-Service Vulnerability
CVE-2017-12240	Cisco	IOS and IOS XE Software	Cisco IOS and IOS XE Software DHCP Remote Code Execution Vulnerability
CVE-2017-12238	Cisco	Catalyst 6800 Series Switches	Cisco Catalyst 6800 Series Switches VPLS Denial-of-Service Vulnerability
CVE-2017-12237	Cisco	IOS and IOS XE Software	Cisco IOS and IOS XE Software Internet Key Exchange Denial-of-Service Vulnerability
CVE-2017-12235	Cisco	IOS software	Cisco IOS Software for Cisco Industrial Ethernet Switches PROFINET Denial-of-Service Vulnerability
CVE-2017-12234	Cisco	IOS software	Cisco IOS Software Common Industrial Protocol Request Denial-of-Service Vulnerability
CVE-2017-12233	Cisco	IOS software	Cisco IOS Software Common Industrial Protocol Request Denial-of-Service Vulnerability
CVE-2017-12232	Cisco	IOS software	Cisco IOS Software for Cisco Integrated Services Routers Denial-of-Service Vulnerability
CVE-2017-12231	Cisco	IOS software	Cisco IOS Software Network Address Translation Denial-of-Service Vulnerability
CVE-2017-11826	Microsoft	Office	Microsoft Office Remote Code Execution Vulnerability
CVE-2017-11292	Adobe	Flash Player	Adobe Flash Player Type Confusion Vulnerability
CVE-2017-0261	Microsoft	Office	Microsoft Office Use-After-Free Vulnerability

CVE-2017-0001	Microsoft	Graphics Device Interface (GDI)	Microsoft Graphics Device Interface (GDI) Privilege Escalation Vulnerability
CVE-2016-8562	Siemens	SIMATIC CP	Siemens SIMATIC CP 1543-1 Improper Privilege Management Vulnerability
CVE-2016-7855	Adobe	Flash Player	Adobe Flash Player Use-After-Free Vulnerability
CVE-2016-7262	Microsoft	Excel	Microsoft Office Security Feature Bypass Vulnerability
CVE-2016-7193	Microsoft	Office	Microsoft Office Memory Corruption Vulnerability
CVE-2016-5195	Linux	Kernel	Linux Kernel Race Condition Vulnerability
CVE-2016-4117	Adobe	Flash Player	Adobe Flash Player Arbitrary Code Execution Vulnerability
CVE-2016-1019	Adobe	Flash Player	Adobe Flash Player Arbitrary Code Execution Vulnerability
CVE-2016-0099	Microsoft	Windows	Microsoft Windows Secondary Logon Service Privilege Escalation Vulnerability
CVE-2015-7645	Adobe	Flash Player	Adobe Flash Player Arbitrary Code Execution Vulnerability
CVE-2015-5119	Adobe	Flash Player	Adobe Flash Player Use-After-Free Vulnerability
CVE-2015-4902	Oracle	Java SE	Oracle Java SE Integrity Check Vulnerability
CVE-2015-3043	Adobe	Flash Player	Adobe Flash Player Memory Corruption Vulnerability
CVE-2015-2590	Oracle	Java SE	Oracle Java SE and Java SE Embedded Remote Code Execution Vulnerability
CVE-2015-2545	Microsoft	Office	Microsoft Office Malformed EPS File Vulnerability
CVE-2015-2424	Microsoft	PowerPoint	Microsoft PowerPoint Memory Corruption Vulnerability
CVE-2015-2387	Microsoft	ATM Font Driver	Microsoft ATM Font Driver Privilege Escalation Vulnerability
CVE-2015-1701	Microsoft	Win32k	Microsoft Win32k Privilege Escalation Vulnerability
CVE-2015-1642	Microsoft	Office	Microsoft Office Memory Corruption Vulnerability
CVE-2014-4114	Microsoft	Windows	Microsoft Windows Object Linking & Embedding (OLE) Remote Code

			Execution Vulnerability
CVE-2014-0496	Adobe	Reader and Acrobat	Adobe Reader and Acrobat Use-After-Free Vulnerability
CVE-2013-5065	Microsoft	Windows	Microsoft Windows Kernel Privilege Escalation Vulnerability
CVE-2013-3897	Microsoft	Internet Explorer	Microsoft Internet Explorer Use-After-Free Vulnerability
CVE-2013-3346	Adobe	Reader and Acrobat	Adobe Reader and Acrobat Memory Corruption Vulnerability
CVE-2013-1675	Mozilla	Firefox	Mozilla Firefox Information Disclosure Vulnerability
CVE-2013-1347	Microsoft	Internet Explorer	Microsoft Internet Explorer Remote Code Execution Vulnerability
CVE-2013-0641	Adobe	Reader	Adobe Reader Buffer Overflow Vulnerability
CVE-2013-0640	Adobe	Reader and Acrobat	Adobe Reader and Acrobat Memory Corruption Vulnerability
CVE-2013-0632	Adobe	ColdFusion	Adobe ColdFusion Authentication Bypass Vulnerability
CVE-2012-4681	Oracle	Java SE	Oracle Java SE Runtime Environment (JRE) Arbitrary Code Execution Vulnerability
CVE-2012-1856	Microsoft	Office	Microsoft Office MSCOMCTL.OCX Remote Code Execution Vulnerability
CVE-2012-1723	Oracle	Java SE	Oracle Java SE Runtime Environment (JRE) Arbitrary Code Execution Vulnerability
CVE-2012-1535	Adobe	Flash Player	Adobe Flash Player Arbitrary Code Execution Vulnerability
CVE-2012-0507	Oracle	Java SE	Oracle Java SE Runtime Environment (JRE) Arbitrary Code Execution Vulnerability
CVE-2011-3544	Oracle	Java SE JDK and JRE	Oracle Java SE Runtime Environment (JRE) Arbitrary Code Execution Vulnerability
CVE-2011-1889	Microsoft	Forefront Threat Management Gateway	Microsoft Forefront TMG Remote Code Execution Vulnerability
CVE-2011-0611	Adobe	Flash Player	Adobe Flash Player Remote Code Execution Vulnerability
CVE-2010-3333	Microsoft	Office	Microsoft Office Stack-based Buffer Overflow Vulnerability

CVE-2010-0232	Microsoft	Windows	Microsoft Windows Kernel Exception Handler Vulnerability
CVE-2010-0188	Adobe	Reader and Acrobat	Adobe Reader and Acrobat Arbitrary Code Execution Vulnerability
CVE-2009-3129	Microsoft	Excel	Microsoft Excel Featheader Record Memory Corruption Vulnerability
CVE-2009-1123	Microsoft	Windows	Microsoft Windows Improper Input Validation Vulnerability
CVE-2008-3431	Oracle	VirtualBox	Oracle VirtualBox Insufficient Input Validation Vulnerability
CVE-2008-2992	Adobe	Acrobat and Reader	Adobe Reader and Acrobat Input Validation Vulnerability
CVE-2004-0210	Microsoft	Windows	Microsoft Windows Privilege Escalation Vulnerability
CVE-2002-0367	Microsoft	Windows	Microsoft Windows Privilege Escalation Vulnerability
CVE-2022-26486	Mozilla	Firefox	Mozilla Firefox Use-After-Free Vulnerability
CVE-2022-26485	Mozilla	Firefox	Mozilla Firefox Use-After-Free Vulnerability
CVE-2021-21973	VMware	vCenter Server and Cloud Foundation	VMware vCenter Server and Cloud Foundation Server Side Request Forgery (SSRF) Vulnerability
CVE-2020-8218	Pulse Secure	Pulse Connect Secure	Pulse Connect Secure Code Injection Vulnerability
CVE-2019-11581	Atlassian	Jira Server and Data Center	Atlassian Jira Server and Data Center Server-Side Template Injection Vulnerability
CVE-2017-6077	NETGEAR	Wireless Router DGN2200	NETGEAR DGN2200 Remote Code Execution Vulnerability
CVE-2016-6277	NETGEAR	Multiple Routers	NETGEAR Multiple Routers Remote Code Execution Vulnerability
CVE-2013-0631	Adobe	ColdFusion	Adobe ColdFusion Information Disclosure Vulnerability
CVE-2013-0629	Adobe	ColdFusion	Adobe ColdFusion Directory Traversal Vulnerability
CVE-2013-0625	Adobe	ColdFusion	Adobe ColdFusion Authentication Bypass Vulnerability
CVE-2009-3960	Adobe	BlazeDS	Adobe BlazeDS Information Disclosure Vulnerability

CVE-2020-5135	SonicWall	SonicOS	SonicWall SonicOS Buffer Overflow Vulnerability
CVE-2019-1405	Microsoft	Windows	Microsoft Windows Universal Plug and Play (UPnP) Service Privilege Escalation Vulnerability
CVE-2019-1322	Microsoft	Windows	Microsoft Windows Privilege Escalation Vulnerability
CVE-2019-1315	Microsoft	Windows	Microsoft Windows Error Reporting Manager Privilege Escalation Vulnerability
CVE-2019-1253	Microsoft	Windows	Microsoft Windows AppX Deployment Server Privilege Escalation Vulnerability
CVE-2019-1132	Microsoft	Win32k	Microsoft Win32k Privilege Escalation Vulnerability
CVE-2019-1129	Microsoft	Windows	Microsoft Windows AppX Deployment Service (AppXSVC) Privilege Escalation Vulnerability
CVE-2019-1069	Microsoft	Task Scheduler	Microsoft Task Scheduler Privilege Escalation Vulnerability
CVE-2019-1064	Microsoft	Windows	Microsoft Windows AppX Deployment Service (AppXSVC) Privilege Escalation Vulnerability
CVE-2019-0841	Microsoft	Windows	Microsoft Windows AppX Deployment Service (AppXSVC) Privilege Escalation Vulnerability
CVE-2019-0543	Microsoft	Windows	Microsoft Windows Privilege Escalation Vulnerability
CVE-2018-8120	Microsoft	Win32k	Microsoft Win32k Privilege Escalation Vulnerability
CVE-2017-0101	Microsoft	Windows	Microsoft Windows Transaction Manager Privilege Escalation Vulnerability
CVE-2016-3309	Microsoft	Windows	Microsoft Windows Kernel Privilege Escalation Vulnerability
CVE-2015-2546	Microsoft	Win32k	Microsoft Win32k Memory Corruption Vulnerability
CVE-2022-26318	WatchGuard	Firebox and XTM Appliances	WatchGuard Firebox and XTM Appliances Arbitrary Code Execution
CVE-2022-26143	Mitel	MiCollab, MiVoice Business Express	MiCollab, MiVoice Business Express Access Control Vulnerability
CVE-2022-21999	Microsoft	Windows	Microsoft Windows Print Spooler Privilege Escalation Vulnerability

CVE-2021-42237	Sitecore	XP	Sitecore XP Remote Command Execution Vulnerability
CVE-2021-22941	Citrix	ShareFile	Citrix ShareFile Improper Access Control Vulnerability
CVE-2020-9377	D-Link	DIR-610 Devices	D-Link DIR-610 Devices Remote Command Execution
CVE-2020-9054	Zyxel	Multiple Network-Attached Storage (NAS) Devices	Zyxel Multiple NAS Devices OS Command Injection Vulnerability
CVE-2020-7247	OpenBSD	OpenSMTPD	OpenSMTPD Remote Code Execution Vulnerability
CVE-2020-5410	VMware Tanzu	Spring Cloud Configuration (Config) Server	VMware Tanzu Spring Cloud Config Directory Traversal Vulnerability
CVE-2020-25223	Sophos	SG UTM	Sophos SG UTM Remote Code Execution Vulnerability
CVE-2020-2506	QNAP Systems	Helpdesk	QNAP Helpdesk Improper Access Control Vulnerability
CVE-2020-2021	Palo Alto	PAN-OS	Palo Alto PAN-OS Authentication Bypass Vulnerability
CVE-2020-1956	Apache	Kylin	Apache Kylin OS Command Injection Vulnerability
CVE-2020-1631	Juniper	Junos OS	Juniper Junos OS Path Traversal Vulnerability
CVE-2019-6340	Drupal	Core	Drupal Core Remote Code Execution Vulnerability
CVE-2019-2616	Oracle	BI Publisher (Formerly XML Publisher)	Oracle BI Publisher Unauthorized Access Vulnerability
CVE-2019-16920	D-Link	Multiple Routers	D-Link Multiple Routers Command Injection Vulnerability
CVE-2019-15107	Webmin	Webmin	Webmin Command Injection Vulnerability
CVE-2019-12991	Citrix	SD-WAN and NetScaler	Citrix SD-WAN and NetScaler Command Injection Vulnerability
CVE-2019-12989	Citrix	SD-WAN and NetScaler	Citrix SD-WAN and NetScaler SQL Injection Vulnerability
CVE-2019-11043	PHP	FastCGI Process Manager (FPM)	PHP FastCGI Process Manager (FPM) Buffer Overflow Vulnerability
CVE-2019-10068	Kentico	Xperience	Kentico Xperience Deserialization of Untrusted Data Vulnerability

CVE-2019-1003030	Jenkins	Matrix Project Plugin	Jenkins Matrix Project Plugin Remote Code Execution Vulnerability
CVE-2019-0903	Microsoft	Graphics Device Interface (GDI)	Microsoft GDI Remote Code Execution Vulnerability
CVE-2018-8414	Microsoft	Windows	Microsoft Windows Shell Remote Code Execution Vulnerability
CVE-2018-8373	Microsoft	Internet Explorer Scripting Engine	Microsoft Scripting Engine Memory Corruption Vulnerability
CVE-2018-6961	VMware	SD-WAN Edge	VMware SD-WAN Edge by VeloCloud Command Injection Vulnerability
CVE-2018-14839	LG	N1A1 NAS	LG N1A1 NAS Remote Command Execution Vulnerability
CVE-2018-1273	VMware Tanzu	Spring Data Commons	VMware Tanzu Spring Data Commons Property Binder Vulnerability
CVE-2018-11138	Quest	KACE System Management Appliance	Quest KACE System Management Appliance Remote Command Execution Vulnerability
CVE-2018-0147	Cisco	Secure Access Control System (ACS)	Cisco Secure Access Control System Java Deserialization Vulnerability
CVE-2018-0125	Cisco	VPN Routers	Cisco VPN Routers Remote Code Execution Vulnerability
CVE-2017-6334	NETGEAR	DGN2200 Devices	NETGEAR DGN2200 Devices OS Command Injection Vulnerability
CVE-2017-6316	Citrix	NetScaler SD-WAN Enterprise, CloudBridge Virtual WAN, and XenMobile Server	Citrix Multiple Products Remote Code Execution Vulnerability
CVE-2017-3881	Cisco	IOS and IOS XE	Cisco IOS and IOS XE Remote Code Execution Vulnerability
CVE-2017-12617	Apache	Tomcat	Apache Tomcat Remote Code Execution Vulnerability
CVE-2017-12615	Apache	Tomcat	Apache Tomcat on Windows Remote Code Execution Vulnerability
CVE-2017-0146	Microsoft	Windows	Microsoft Windows SMB Remote Code Execution Vulnerability
CVE-2016-7892	Adobe	Flash Player	Adobe Flash Player Use-After-Free Vulnerability
CVE-2016-4171	Adobe	Flash Player	Adobe Flash Player Remote Code Execution Vulnerability
CVE-2016-1555	NETGEAR	Wireless Access Point (WAP) Devices	NETGEAR Multiple WAP Devices Command Injection Vulnerability

CVE-2016-11021	D-Link	DCS-930L Devices	D-Link DCS-930L Devices OS Command Injection Vulnerability
CVE-2016-10174	NETGEAR	WNR2000v5 Router	NETGEAR WNR2000v5 Router Buffer Overflow Vulnerability
CVE-2016-0752	Rails	Ruby on Rails	Ruby on Rails Directory Traversal Vulnerability
CVE-2015-4068	Arcserve	Unified Data Protection (UDP)	Arcserve Unified Data Protection (UDP) Directory Traversal Vulnerability
CVE-2015-3035	TP-Link	Multiple Archer Devices	TP-Link Multiple Archer Devices Directory Traversal Vulnerability
CVE-2015-1427	Elastic	Elasticsearch	Elasticsearch Groovy Scripting Engine Remote Code Execution Vulnerability
CVE-2015-1187	D-Link and TRENDnet	Multiple Devices	D-Link and TRENDnet Multiple Devices Remote Code Execution Vulnerability
CVE-2015-0666	Cisco	Prime Data Center Network Manager (DCNM)	Cisco Prime Data Center Network Manager (DCNM) Directory Traversal Vulnerability
CVE-2014-6332	Microsoft	Windows	Microsoft Windows Object Linking & Embedding (OLE) Automation Array Remote Code Execution Vulnerability
CVE-2014-6324	Microsoft	Kerberos Key Distribution Center (KDC)	Microsoft Kerberos Key Distribution Center (KDC) Privilege Escalation Vulnerability
CVE-2014-6287	Rejetto	HTTP File Server (HFS)	Rejetto HTTP File Server (HFS) Remote Code Execution Vulnerability
CVE-2014-3120	Elastic	Elasticsearch	Elasticsearch Remote Code Execution Vulnerability
CVE-2014-0130	Rails	Ruby on Rails	Ruby on Rails Directory Traversal Vulnerability
CVE-2013-5223	D-Link	DSL-2760U	D-Link DSL-2760U Gateway Cross-Site Scripting Vulnerability
CVE-2013-4810	Hewlett Packard (HP)	ProCurve Manager (PCM), PCM+, Identity Driven Manager (IDM), and Application Lifecycle Management	HP Multiple Products Remote Code Execution Vulnerability
CVE-2013-2251	Apache	Struts	Apache Struts Improper Input Validation Vulnerability
CVE-2012-1823	PHP	PHP	PHP-CGI Query String Parameter Vulnerability

CVE-2010-4345	Exim	Exim	Exim Privilege Escalation Vulnerability
CVE-2010-4344	Exim	Exim	Exim Heap-Based Buffer Overflow Vulnerability
CVE-2010-3035	Cisco	IOS XR	Cisco IOS XR Border Gateway Protocol (BGP) Denial-of-Service Vulnerability
CVE-2010-2861	Adobe	ColdFusion	Adobe ColdFusion Directory Traversal Vulnerability
CVE-2009-2055	Cisco	IOS XR	Cisco IOS XR Border Gateway Protocol (BGP) Denial-of-Service Vulnerability
CVE-2009-1151	phpMyAdmin	phpMyAdmin	phpMyAdmin Remote Code Execution Vulnerability
CVE-2009-0927	Adobe	Reader and Acrobat	Adobe Reader and Adobe Acrobat Stack-Based Buffer Overflow Vulnerability
CVE-2005-2773	Hewlett Packard (HP)	OpenView Network Node Manager	HP OpenView Network Node Manager Remote Code Execution Vulnerability
CVE-2022-1096	Google	Chromium V8	Google Chromium V8 Type Confusion Vulnerability
CVE-2022-0543	Redis	Debian-specific Redis Servers	Debian-specific Redis Server Lua Sandbox Escape Vulnerability
CVE-2021-38646	Microsoft	Office	Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability
CVE-2021-34486	Microsoft	Windows	Microsoft Windows Event Tracing Privilege Escalation Vulnerability
CVE-2021-26085	Atlassian	Confluence Server	Atlassian Confluence Server Pre-Authorization Arbitrary File Read Vulnerability
CVE-2021-20028	SonicWall	Secure Remote Access (SRA)	SonicWall Secure Remote Access (SRA) SQL Injection Vulnerability
CVE-2019-7483	SonicWall	SMA100	SonicWall SMA100 Directory Traversal Vulnerability
CVE-2018-8440	Microsoft	Windows	Microsoft Windows Privilege Escalation Vulnerability
CVE-2018-8406	Microsoft	DirectX Graphics Kernel (DXGKRNL)	Microsoft DirectX Graphics Kernel Privilege Escalation Vulnerability
CVE-2018-8405	Microsoft	DirectX Graphics Kernel (DXGKRNL)	Microsoft DirectX Graphics Kernel Privilege Escalation Vulnerability
CVE-2017-0213	Microsoft	Windows	Microsoft Windows Privilege Escalation Vulnerability

CVE-2017-0059	Microsoft	Internet Explorer	Microsoft Internet Explorer Information Disclosure Vulnerability
CVE-2017-0037	Microsoft	Edge and Internet Explorer	Microsoft Edge and Internet Explorer Type Confusion Vulnerability
CVE-2016-7201	Microsoft	Edge	Microsoft Edge Memory Corruption Vulnerability
CVE-2016-7200	Microsoft	Edge	Microsoft Edge Memory Corruption Vulnerability
CVE-2016-0189	Microsoft	Internet Explorer	Microsoft Internet Explorer Memory Corruption Vulnerability
CVE-2016-0151	Microsoft	Client-Server Run-time Subsystem (CSRSS)	Microsoft Windows CSRSS Security Feature Bypass Vulnerability
CVE-2016-0040	Microsoft	Windows	Microsoft Windows Kernel Privilege Escalation Vulnerability
CVE-2015-2426	Microsoft	Windows	Microsoft Windows Adobe Type Manager Library Remote Code Execution Vulnerability
CVE-2015-2419	Microsoft	Internet Explorer	Microsoft Internet Explorer Memory Corruption Vulnerability
CVE-2015-1770	Microsoft	Office	Microsoft Office Uninitialized Memory Use Vulnerability
CVE-2013-3660	Microsoft	Win32k	Microsoft Win32k Privilege Escalation Vulnerability
CVE-2013-2729	Adobe	Reader and Acrobat	Adobe Reader and Acrobat Arbitrary Integer Overflow Vulnerability
CVE-2013-2551	Microsoft	Internet Explorer	Microsoft Internet Explorer Use-After-Free Vulnerability
CVE-2013-2465	Oracle	Java SE	Oracle Java SE Unspecified Vulnerability
CVE-2013-1690	Mozilla	Firefox and Thunderbird	Mozilla Firefox and Thunderbird Denial-of-Service Vulnerability
CVE-2012-5076	Oracle	Java SE	Oracle Java SE Sandbox Bypass Vulnerability
CVE-2012-2539	Microsoft	Word	Microsoft Word Remote Code Execution Vulnerability
CVE-2012-2034	Adobe	Flash Player	Adobe Flash Player Memory Corruption Vulnerability
CVE-2012-0518	Oracle	Fusion Middleware	Oracle Fusion Middleware Unspecified Vulnerability

CVE-2011-2005	Microsoft	Ancillary Function Driver (afd.sys)	Microsoft Ancillary Function Driver (afd.sys) Improper Input Validation Vulnerability
CVE-2010-4398	Microsoft	Windows	Microsoft Windows Kernel Stack-Based Buffer Overflow Vulnerability
CVE-2022-26871	Trend Micro	Apex Central	Trend Micro Apex Central Arbitrary File Upload Vulnerability
CVE-2022-1040	Sophos	Firewall	Sophos Firewall Authentication Bypass Vulnerability
CVE-2021-34484	Microsoft	Windows	Microsoft Windows User Profile Service Privilege Escalation Vulnerability
CVE-2021-28799	QNAP	Network Attached Storage (NAS)	QNAP NAS Improper Authorization Vulnerability
CVE-2021-21551	Dell	dbutil Driver	Dell dbutil Driver Insufficient Access Control Vulnerability
CVE-2018-10562	Dasan	Gigabit Passive Optical Network (GPON) Routers	Dasan GPON Routers Command Injection Vulnerability
CVE-2018-10561	Dasan	Gigabit Passive Optical Network (GPON) Routers	Dasan GPON Routers Authentication Bypass Vulnerability
CVE-2022-22965	Vmware	Spring Framework	Spring Framework JDK 9+ Remote Code Execution Vulnerability
CVE-2022-22675	Apple	macOS	Apple macOS Out-of-Bounds Write Vulnerability
CVE-2022-22674	Apple	macOS	Apple macOS Out-of-Bounds Read Vulnerability
CVE-2021-45382	D-Link	Multiple Routers	D-Link Multiple Routers Remote Code Execution Vulnerability