



## Vulnerabilities

On this page you can find vulnerabilities, security advisories, exploit codes and proof-of-concept codes discovered by Zero Science Lab team.



### - 2022 -

- [14.12.2022] SOUND4 IMPACT/FIRST/PULSE/Eco <=2.x (restorefactory.cgi) Factory Reset
- [14.12.2022] SOUND4 IMPACT/FIRST/PULSE/Eco <=2.x (upload.cgi) Unauthenticated Code Execution
- [14.12.2022] SOUND4 IMPACT/FIRST/PULSE/Eco <=2.x (traceroute.php) Conditional Command Injection
- [14.12.2022] SOUND4 IMPACT/FIRST/PULSE/Eco <=2.x (username) Command Injection
- [14.12.2022] SOUND4 IMPACT/FIRST/PULSE/Eco <=2.x (password) Unauthenticated Command Injection
- [14.12.2022] SOUND4 IMPACT/FIRST/PULSE/Eco <=2.x (services) Authenticated Command Injection
- [14.12.2022] SOUND4 IMPACT/FIRST/PULSE/Eco <=2.x (PHPTail) Unauthenticated File Disclosure
- [14.12.2022] SOUND4 IMPACT/FIRST/PULSE/Eco <=2.x (ping.php) Conditional Command Injection
- [14.12.2022] SOUND4 IMPACT/FIRST/PULSE/Eco <=2.x Unauthenticated Radio Stream Disclosure
- [14.12.2022] SOUND4 IMPACT/FIRST/PULSE/Eco <=2.x (dns.php) Conditional Command Injection
- [14.12.2022] SOUND4 IMPACT/FIRST/PULSE/Eco <=2.x (Index of /log) Information Disclosure
- [14.12.2022] SOUND4 IMPACT/FIRST/PULSE/Eco <=2.x (username) Stored Cross-Site Scripting
- [14.12.2022] SOUND4 IMPACT/FIRST/PULSE/Eco <=2.x Directory Traversal File Write Exploit
- [14.12.2022] SOUND4 IMPACT/FIRST/PULSE/Eco <=2.x (sound4server) Hardcoded Credentials
- [14.12.2022] SOUND4 IMPACT/FIRST/PULSE/Eco <=2.x (ping/traceroute) ICMP Flood Attack
- [14.12.2022] SOUND4 IMPACT/FIRST/PULSE/Eco <=2.x (username) Authentication Bypass
- [14.12.2022] SOUND4 IMPACT/FIRST/PULSE/Eco <=2.x (password) Authentication Bypass
- [14.12.2022] SOUND4 IMPACT/FIRST/PULSE/Eco <=2.x Disconnect Webmonitor User (DoS)
- [14.12.2022] SOUND4 IMPACT/FIRST/PULSE/Eco <=2.x Insufficient Session Expiration
- [14.12.2022] SOUND4 IMPACT/FIRST/PULSE/Eco <=2.x Authorization Bypass (IDOR)
- [14.12.2022] SOUND4 IMPACT/FIRST/PULSE/Eco <=2.x Cross-Site Request Forgery
- [14.12.2022] SOUND4 Server Service 4.1.102 Local Privilege Escalation
- [09.12.2022] Spitfire CMS 1.0.475 (cms\_backup\_values) PHP Object Injection
- [16.10.2022] MiniDVBLinux 5.4 Arbitrary File Read Vulnerability
- [16.10.2022] MiniDVBLinux 5.4 Remote Root Command Execution Vulnerability
- [16.10.2022] MiniDVBLinux 5.4 Remote Root Command Injection Vulnerability
- [16.10.2022] MiniDVBLinux 5.4 Unauthenticated Stream Disclosure Vulnerability
- [16.10.2022] MiniDVBLinux 5.4 Change Root Password PoC
- [16.10.2022] MiniDVBLinux 5.4 Simple VideoDiskRecorder Protocol SVDPR (svdrpsend.sh) Exploit
- [16.10.2022] MiniDVBLinux 5.4 Config Download Exploit
- [18.09.2022] SoX 14.4.2 (wav.c) Division By Zero
- [11.09.2022] ETAP Safety Manager 1.0.0.32 Remote Unauthenticated Reflected XSS
- [20.07.2022] Schneider Electric SpaceLogic C-Bus Home Controller (5200WHC2) Remote Root Exploit
- [30.06.2022] Carel pCOWeb HVAC BACnet Gateway 2.1.0 Unauthenticated Directory Traversal
- [14.06.2022] JM-DATA ONU JF511-TV Multiple Remote Vulnerabilities
- [29.05.2022] Schneider Electric C-Bus Automation Controller (5500SHAC) 1.10 Remote Root Exploit
- [03.05.2022] Tenda HG6 v3.3.0 Remote Command Injection Vulnerability
- [20.04.2022] USR IOT 4G LTE Industrial Cellular VPN Router 1.0.36 Remote Root Backdoor
- [14.04.2022] Delta Controls enteliTOUCH 3.40.3935 Cookie User Password Disclosure
- [14.04.2022] Delta Controls enteliTOUCH 3.40.3935 Cross-Site Scripting (XSS)
- [14.04.2022] Delta Controls enteliTOUCH 3.40.3935 Cross-Site Request Forgery (CSRF)
- [13.04.2022] Verizon 4G LTE Network Extender Weak Credentials Algorithm
- [21.03.2022] ICT Protege GX/WX 2.08 Client-Side SHA1 Password Hash Disclosure
- [21.03.2022] ICT Protege GX/WX 2.08 Authenticated Stored XSS Vulnerability
- [22.02.2022] ICL ScadaFlex II SCADA Controllers SC-1/SC-2 1.03.07 Remote File CRUD
- [12.02.2022] H3C SSL VPN Username Enumeration
- [27.01.2022] Fetch Softworks Fetch FTP Client 5.8 Remote CPU Consumption (Denial of Service)
- [16.01.2022] OpenBMCS 2.4 Secrets Disclosure
- [16.01.2022] OpenBMCS 2.4 Unauthenticated SSRF / RFI
- [16.01.2022] OpenBMCS 2.4 Create Admin / Remote Privilege Escalation
- [16.01.2022] OpenBMCS 2.4 Authenticated SQL Injection
- [16.01.2022] OpenBMCS 2.4 CSRF Send E-mail

### - 2021 -

- [13.12.2021] meterN v1.2.3 Authenticated Remote Command Execution Vulnerability
- [13.12.2021] Zucchetti Axess CLOKI Access Control 1.64 CSRF Disable Access Control
- [01.11.2021] i3 International Annexus Cameras Ax-n 5.2.0 Application Logic Flaw
- [10.10.2021] Cypress Solutions CTM-200 2.7.1 Root Remote OS Command Injection

- [10.10.2021] Cypress Solutions CTM-200/CTM-ONE Hard-coded Credentials Remote Root (Telnet/SSH)
- [27.09.2021] FatPipe Networks WARP/IPVPN/MPVPN 10.2.2 Remote Privilege Escalation
- [27.09.2021] FatPipe Networks WARP/IPVPN/MPVPN 10.2.2 Hidden Backdoor Account (Write Access)
- [27.09.2021] FatPipe Networks WARP/IPVPN/MPVPN 10.2.2 Unauthenticated Config Download
- [27.09.2021] FatPipe Networks WARP 10.2.2 Authorization Bypass
- [27.09.2021] FatPipe Networks WARP/IPVPN/MPVPN 10.2.2 CSRF Add Admin Exploit
- [09.09.2021] ECOA Building Automation System Arbitrary File Deletion
- [09.09.2021] ECOA Building Automation System Local File Disclosure Vulnerability
- [09.09.2021] ECOA Building Automation System Authorization Bypass / IDOR
- [09.09.2021] ECOA Building Automation System Remote Privilege Escalation
- [09.09.2021] ECOA Building Automation System Missing Encryption Of Sensitive Information
- [08.09.2021] ECOA Building Automation System Hard-coded Credentials SSH Access
- [08.09.2021] ECOA Building Automation System Hidden Backdoor Accounts and backdoor() Function
- [08.09.2021] ECOA Building Automation System Configuration Download Information Disclosure
- [08.09.2021] ECOA Building Automation System Cookie Poisoning Authentication Bypass
- [08.09.2021] ECOA Building Automation System Cross-Site Request Forgery
- [08.09.2021] ECOA Building Automation System Directory Traversal Content Disclosure
- [08.09.2021] ECOA Building Automation System Path Traversal Arbitrary File Upload
- [08.09.2021] ECOA Building Automation System Weak Default Credentials
- [15.08.2021] COMMAX CVD-Axx DVR 5.1.4 Weak Default Credentials Stream Disclosure
- [15.08.2021] COMMAX Smart Home Ruvie CCTV Bridge DVR Service Unauthenticated Config Write / DoS
- [15.08.2021] COMMAX Smart Home Ruvie CCTV Bridge DVR Service RTSP Credentials Disclosure
- [15.08.2021] COMMAX UMS Client ActiveX Control 1.7.0.2 (CNC\_Ctrl.dll) Heap Buffer Overflow
- [15.08.2021] COMMAX WebViewer ActiveX Control 2.1.4.5 (Commax\_WebViewer.ocx) Buffer Overflow
- [15.08.2021] COMMAX Smart Home IoT Control System CDP-1020n SQL Injection Authentication Bypass
- [15.08.2021] COMMAX Biometric Access Control System 1.0.0 Authentication Bypass
- [15.08.2021] COMMAX Biometric Access Control System 1.0.0 Cookie Reflected XSS
- [30.07.2021] Panasonic Sanyo CCTV Network Camera 2.03 CSRF Disable Auth / Change Password
- [28.07.2021] IntelliChoice eFORCE Software Suite v2.5.9 Username Enumeration
- [28.07.2021] Longjing Technology BEMS API 1.21 Remote Arbitrary File Download
- [20.07.2021] KevinLAB BEMS 1.0 Authenticated File Path Traversal Information Disclosure
- [20.07.2021] KevinLAB BEMS 1.0 Unauthenticated SQL Injection / Authentication Bypass
- [20.07.2021] KevinLAB BEMS 1.0 Undocumented Backdoor Account
- [04.07.2021] Ricon Industrial Cellular Router S9922XL Remote Command Execution
- [06.05.2021] Epic Games Easy Anti-Cheat 4.0 Local Privilege Escalation
- [30.04.2021] Epic Games Rocket League 1.95 (AK::MemoryMgr::GetPoolName) Stack Buffer Overrun
- [30.04.2021] Epic Games Psyonix Rocket League <=1.95 Insecure Permissions
- [23.04.2021] Sipwise C5 NGCP CSC CSRF Click2Dial Exploit
- [23.04.2021] Sipwise C5 NGCP CSC Multiple Stored/Reflected XSS Vulnerabilities
- [01.04.2021] ZBL EPON ONU Broadband Router 1.0 Remote Privilege Escalation Exploit
- [18.03.2021] KZTech/JatonTec/Neotel JT3500V 4G LTE CPE 2.0.1 Insufficient Session Expiration
- [18.03.2021] KZTech/JatonTec/Neotel JT3500V 4G LTE CPE 2.0.1 Privilege Escalation
- [18.03.2021] KZTech/JatonTec/Neotel JT3500V 4G LTE CPE 2.0.1 Unauthenticated Config Download
- [18.03.2021] KZTech/JatonTec/Neotel JT3500V 4G LTE CPE 2.0.1 Unauthenticated Device Reboot (DoS)
- [18.03.2021] KZTech/JatonTec/Neotel JT3500V 4G LTE CPE 2.0.1 Unauthenticated Factory Reset
- [18.03.2021] KZTech/JatonTec/Neotel JT3500V 4G LTE CPE 2.0.1 Unauthenticated Log Disclosure
- [18.03.2021] KZTech/JatonTec/Neotel JT3500V 4G LTE CPE 2.0.1 Improper Access Control (IDOR)
- [18.03.2021] KZTech/JatonTec/Neotel JT3500V 4G LTE CPE 2.0.1 Remote Code Execution (Backdoors)
- [18.03.2021] KZTech/JatonTec/Neotel JT3500V 4G LTE CPE 2.0.1 Weak Default WiFi Password Algorithm
- [18.03.2021] KZTech/JatonTec/Neotel JT3500V 4G LTE CPE 2.0.1 Hard-coded Credentials Shell Access
- [18.03.2021] KZTech/JatonTec/Neotel JT3500V 4G LTE CPE 2.0.1 Authentication Bypass
- [18.03.2021] KZTech/JatonTec/Neotel JT3500V 4G LTE CPE 2.0.1 Authenticated Command Injection
- [18.03.2021] SOYAL 701Client 9.0.1 Insecure Permissions
- [18.03.2021] SOYAL 701Server 9.0.1 Insecure Permissions
- [18.03.2021] SOYAL Biometric Access Control System 5.0 CSRF Change Admin Password
- [18.03.2021] SOYAL Biometric Access Control System 5.0 Weak Default Credentials
- [18.03.2021] SOYAL Biometric Access Control System 5.0 Master Code Disclosure
- [10.03.2021] NuCom 11N Wireless Router v5.07.90 Remote Privilege Escalation
- [07.02.2021] SmartFoxServer 2X 2.17.0 God Mode Console Remote Code Execution
- [07.02.2021] SmartFoxServer 2X 2.17.0 Credentials Disclosure
- [07.02.2021] SmartFoxServer 2X 2.17.0 God Mode Console WebSocket XSS
- [26.01.2021] STVS ProVision 5.9.10 Cross-Site Request Forgery (Add Admin)
- [26.01.2021] STVS ProVision 5.9.10 Authenticated Reflected Cross-Site Scripting
- [26.01.2021] STVS ProVision 5.9.10 (archive.rb) Authenticated File Disclosure Vulnerability
- [21.01.2021] Selea CarPlateServer (CPS) v4.0.1.6 Remote Program Execution
- [21.01.2021] Selea CarPlateServer (CPS) v4.0.1.6 Local Privilege Escalation
- [21.01.2021] Selea Targa IP OCR-ANPR Camera Unauthenticated Remote Code Execution
- [21.01.2021] Selea Targa IP OCR-ANPR Camera Unauthenticated RTP/RTSP/M-JPEG Stream Disclosure
- [21.01.2021] Selea Targa IP OCR-ANPR Camera CSRF Add Admin Exploit
- [21.01.2021] Selea Targa IP OCR-ANPR Camera Unauthenticated SSRF
- [21.01.2021] Selea Targa IP OCR-ANPR Camera Unauthenticated Directory Traversal File Disclosure
- [21.01.2021] Selea Targa IP OCR-ANPR Camera Developer Backdoor Config Overwrite
- [21.01.2021] Selea Targa IP OCR-ANPR Camera Remote Stored XSS

## - 2020 -

- [24.12.2020] Arteco Web Client DVR/NVR 'SessionId' Cookie Brute Force Session Hijacking Exploit
- [02.12.2020] Sony BRAVIA Digital Signage 1.7.8 Unauthenticated Remote File Inclusion
- [02.12.2020] Sony BRAVIA Digital Signage 1.7.8 Client-Side Protection Bypass / IDOR
- [02.12.2020] Sony BRAVIA Digital Signage 1.7.8 System API Information Disclosure
- [15.11.2020] RED-V Super Digital Signage System RXV-A740R Log Information Disclosure
- [04.11.2020] IDS6 DSSPro Digital Signage System 6.2 Improper Access Control Privilege Escalation
- [04.11.2020] IDS6 DSSPro Digital Signage System 6.2 CAPTCHA Security Bypass
- [04.11.2020] IDS6 DSSPro Digital Signage System 6.2 Cross-Site Request Forgery (CSRF)
- [04.11.2020] IDS6 DSSPro Digital Signage System 6.2 (autoSave) Cookie User Password Disclosure
- [26.10.2020] TDM Digital Signage PC Player 4.1 Insecure File Permissions
- [26.10.2020] Adtec Digital Multiple Products Default/Hardcoded Credentials Remote Root
- [18.10.2020] ReQuest Serious Play F3 Media Server 7.0.3 Unauthenticated Remote Code Execution
- [18.10.2020] ReQuest Serious Play F3 Media Server 7.0.3 Remote Denial of Service
- [18.10.2020] ReQuest Serious Play F3 Media Server 7.0.3 Debug Log Disclosure
- [18.10.2020] ReQuest Serious Play Media Player 3.0 Directory Traversal File Disclosure Vulnerability
- [06.10.2020] EmbedThis GoAhead Web Server 5.1.1 Digest Authentication Capture Replay Nonce Reuse
- [06.10.2020] BACnet Test Server 1.01 Remote Denial of Service Exploit
- [30.09.2020] Sony IPELA Network Camera (ftpcient.cgi) Remote Stack Buffer Overflow

- [30.09.2020] BrightSign Digital Signage Diagnostic Web Server 8.2.26 Unauthenticated SSRF
- [30.09.2020] SpinetiX Fusion Digital Signage 3.4.8 File Backup/Delete Path Traversal
- [30.09.2020] SpinetiX Fusion Digital Signage 3.4.8 Database Backup Disclosure
- [30.09.2020] SpinetiX Fusion Digital Signage 3.4.8 CSRF Add Admin Exploit
- [30.09.2020] SpinetiX Fusion Digital Signage 3.4.8 Username Enumeration Weakness
- [19.09.2020] B-swiss 3 Digital Signage System 3.6.5 Backdoor Remote Code Execution
- [19.09.2020] B-swiss 3 Digital Signage System 3.6.5 CSRF Add Maintenance Admin
- [19.09.2020] B-swiss 3 Digital Signage System 3.6.5 Database Disclosure
- [06.09.2020] Rapid7 Nexpose Installer 6.6.39 Local Privilege Escalation
- [21.08.2020] Eibiz i-Media Server Digital Signage 3.8.0 (createUser) Authentication Bypass (Add Admin)
- [21.08.2020] Eibiz i-Media Server Digital Signage 3.8.0 (oldfile) File Path Traversal
- [21.08.2020] Eibiz i-Media Server Digital Signage 3.8.0 Remote Privilege Escalation / Account Takeover
- [21.08.2020] Eibiz i-Media Server Digital Signage 3.8.0 Configuration Disclosure
- [13.08.2020] QiHang Media Web (QH.aspx) Digital Signage 3.0.9 (pre-auth) Remote Code Execution
- [13.08.2020] QiHang Media Web (QH.aspx) Digital Signage 3.0.9 Arbitrary File Disclosure Vulnerability
- [13.08.2020] QiHang Media Web (QH.aspx) Digital Signage 3.0.9 Unauthenticated Arbitrary File Deletion
- [13.08.2020] QiHang Media Web (QH.aspx) Digital Signage 3.0.9 Cleartext Credentials Disclosure
- [13.08.2020] QiHang Media Web (QH.aspx) Digital Signage 3.0.9 Cookie User Password Disclosure
- [31.07.2020] All-Dynamics Software enlogic:show Digital Signage System 2.0.2 Session Fixation
- [31.07.2020] All-Dynamics Software enlogic:show Digital Signage System 2.0.2 CSRF Add Admin
- [19.07.2020] UBICOD Medivision Digital Signage 1.5.1 Privilege Escalation Through Authorization Bypass
- [19.07.2020] UBICOD Medivision Digital Signage 1.5.1 CSRF Add Super Admin
- [19.07.2020] Plexus anblick Digital Signage Management 3.1.13 (pagina param) Open Redirect
- [05.07.2020] rauLink Software Domotica Web 2.0 SQL Injection Authentication Bypass
- [04.06.2020] Cayin Digital Signage System xPost 2.5 Pre-Auth SQLi Remote Code Execution
- [04.06.2020] Cayin Content Management Server 11.0 Root Remote Command Injection
- [04.06.2020] Cayin Signage Media Player 3.0 Root Remote Command Injection
- [04.06.2020] Secure Computing SnapGear Management Console SG560 v3.1.5 Arbitrary File Read/Write
- [04.06.2020] Secure Computing SnapGear Management Console SG560 v3.1.5 CSRF Add Super User
- [05.05.2020] Extreme Networks Aerohive HiveOS <=11.x Remote Denial of Service Exploit
- [24.04.2020] Furukawa Electric ConsciusMAP 2.8.1 Java Deserialization Remote Code Execution
- [21.04.2020] P5 FNIP-8x16A/FNIP-4xSH CSRF Stored Cross-Site Scripting
- [22.03.2020] FIBARO System Home Center v5.021 Remote File Include XSS
- [15.02.2020] Nanometrics Centaur / TitanSMA Unauthenticated Remote Memory Leak Exploit
- [28.01.2020] Fifthplay S.A.M.I - Service And Management Interface Unauthenticated Stored XSS

## - 2019 -

- [29.12.2019] HomeAutomation v3.3.2 CSRF Remote Command Execution (PHP Reverse Shell) PoC
- [29.12.2019] HomeAutomation v3.3.2 Open Redirect
- [29.12.2019] HomeAutomation v3.3.2 CSRF Add Admin Exploit
- [29.12.2019] HomeAutomation v3.3.2 Authentication Bypass Exploit
- [29.12.2019] HomeAutomation v3.3.2 Stored and Reflected XSS
- [29.12.2019] MyDomoAtHome (MDAH) REST API Domoticz ISS Gateway 0.2.40 Information Disclosure
- [29.12.2019] Thrive Smart Home v1.1 SQL Injection Authentication Bypass
- [29.12.2019] Thrive Smart Home v1.1 Reflected Cross-Site Scripting
- [29.12.2019] WEMS BEMS 21.3.1 Undocumented Backdoor Account
- [29.12.2019] WEMS Enterprise Manager 2.58 (email) Reflected XSS
- [27.12.2019] AVE DOMINApus <=1.10.x Credentials Disclosure Exploit
- [27.12.2019] AVE DOMINApus <=1.10.x Authentication Bypass Exploit
- [27.12.2019] AVE DOMINApus <=1.10.x Unauthenticated Remote Reboot
- [27.12.2019] AVE DOMINApus <=1.10.x CSRF/XSS Vulnerabilities
- [09.12.2019] Inim Electronics Smartliving SmartLAN/G/SI <=6.x Hard-coded Credentials
- [09.12.2019] Inim Electronics Smartliving SmartLAN/G/SI <=6.x Unauthenticated SSRF
- [09.12.2019] Inim Electronics SmartLiving SmartLAN/G/SI <=6.x Root Remote Command Execution
- [30.11.2019] Carlo Gavazzi SmartHouse Webapp 6.5.33 CSRF/XSS Vulnerabilities
- [13.11.2019] Siemens Desigo PX V6.00 Web Remote Denial of Service Exploit
- [05.11.2019] Smartwares HOME easy v1.0.9 Database Backup Information Disclosure Exploit
- [05.11.2019] Smartwares HOME easy v1.0.9 Client-Side Authentication Bypass
- [29.10.2019] iSeeQ Hybrid DVR WH-H4 1.03R / 2.0.0.P (get\_jpeg) Stream Disclosure
- [26.09.2019] V-SOL GPON/EPON OLT Platform v2.03 Remote Privilege Escalation
- [26.09.2019] V-SOL GPON/EPON OLT Platform v2.03 Reflected XSS Vulnerability
- [26.09.2019] V-SOL GPON/EPON OLT Platform v2.03 Cross-Site Request Forgery
- [26.09.2019] V-SOL GPON/EPON OLT Platform v2.03 Link Manipulation Vulnerability
- [26.09.2019] V-SOL GPON/EPON OLT Platform v2.03 Unauthenticated Configuration Download
- [24.09.2019] Microsoft SharePoint 2013 SP1 Stored XSS Vulnerability
- [08.09.2019] Rifatron Intelligent Digital Security System (animate.cgi) Stream Disclosure
- [24.07.2019] Yahei-PHP Prober v0.4.7 (speed) Remote HTML Injection Vulnerability
- [18.07.2019] WordPress Plugin OneSignal 1.17.5 Persistent Cross-Site Scripting
- [30.06.2019] FaceSentry Access Control System 6.4.8 Cleartext Password Storage
- [30.06.2019] FaceSentry Access Control System 6.4.8 Authentication Credentials MiTM Disclosure
- [30.06.2019] FaceSentry Access Control System 6.4.8 Reflected Cross-Site Scripting
- [30.06.2019] FaceSentry Access Control System 6.4.8 Remote SSH Root Access Exploit
- [30.06.2019] FaceSentry Access Control System 6.4.8 Remote Root Exploit
- [30.06.2019] FaceSentry Access Control System 6.4.8 Cross-Site Request Forgery
- [30.06.2019] FaceSentry Access Control System 6.4.8 Remote Command Injection
- [15.05.2019] Legrand BTicino Driver Manager F454 1.0.51 Authenticated Stored XSS Exploit
- [15.05.2019] Legrand BTicino Driver Manager F454 1.0.51 CSRF Change Password Exploit
- [13.05.2019] SOCA Access Control System 180612 CSRF Add Admin Exploit
- [13.05.2019] SOCA Access Control System 180612 SQL Injection And Authentication Bypass
- [13.05.2019] SOCA Access Control System 180612 Reflected Cross-Site Scripting
- [13.05.2019] SOCA Access Control System 180612 Information Disclosure
- [23.04.2019] Ross Video DashBoard 8.5.1 Insecure Permissions
- [18.03.2019] exacqVision 9.8 Unquoted Service Path Privilege Escalation
- [13.03.2019] Intel Modular Server System 10.18 CSRF Change Admin Password Exploit
- [09.03.2019] NREL BEopt 2.8.0 Insecure Library Loading Arbitrary Code Execution
- [04.02.2019] BEWARD N100 H.264 VGA IP Camera M2.1.6 Root Remote Code Execution
- [04.02.2019] BEWARD N100 H.264 VGA IP Camera M2.1.6 Arbitrary File Disclosure
- [04.02.2019] BEWARD N100 H.264 VGA IP Camera M2.1.6 CSRF Add Admin Exploit
- [04.02.2019] BEWARD N100 H.264 VGA IP Camera M2.1.6 Unauthenticated RTSP Stream Disclosure
- [03.02.2019] devolo dLAN 550 duo+ Starter Kit Remote Code Execution
- [03.02.2019] devolo dLAN 550 duo+ Starter Kit Cross-Site Request Forgery
- [03.02.2019] devolo dLAN Cockpit 4.3.1 Unquoted Service Path Privilege Escalation
- [27.01.2019] BEWARD Intercom 2.3.1 Credentials Disclosure

- [18.01.2019] ManageEngine OpManager Privilege Escalation
- [05.01.2019] Leica Geosystems GR10/GR25/GR30/GR50 GNSS 4.30.063 JS/HTML Code Injection
- [05.01.2019] Leica Geosystems GR10/GR25/GR30/GR50 GNSS 4.30.063 Cross-Site Request Forgery

## - 2018 -

- [17.11.2018] Synaccess netBooter NP-0801DU 7.4 CSRF Add Admin Exploit
- [17.11.2018] Synaccess netBooter NP-02x/NP-08x 6.8 Authentication Bypass
- [03.11.2018] Microsoft Internet Explorer 11 Tree::Notify\_InvalidateDisplay Null Pointer Dereference
- [01.11.2018] Anviz AIM CrossChex Standard 4.3 Excel Macro Injection
- [17.10.2018] TP-Link TL-SC3130 1.6.18 Unauthenticated RTSP Stream Disclosure Vulnerability
- [14.10.2018] FLIR Systems FLIR Brickstream 3D+ Unauthenticated RTSP Stream Disclosure
- [14.10.2018] FLIR Systems FLIR Brickstream 3D+ Unauthenticated Config Download File Disclosure
- [14.10.2018] FLIR Systems FLIR AX8 Thermal Camera 1.32.16 Hard-coded Credentials Shell Access
- [14.10.2018] FLIR Systems FLIR AX8 Thermal Camera 1.32.16 Arbitrary File Disclosure
- [14.10.2018] FLIR Systems FLIR AX8 Thermal Camera 1.32.16 RTSP Stream Disclosure
- [14.10.2018] FLIR Systems FLIR AX8 Thermal Camera 1.32.16 Remote Root Exploit
- [06.10.2018] FLIR Systems FLIR Thermal Traffic Cameras Websocket Device Manipulation
- [06.10.2018] FLIR Systems FLIR Thermal Traffic Cameras RTSP Stream Disclosure
- [05.09.2018] NovaRad NovaPACS Diagnostics Viewer v8.5 OOB XXE File Disclosure
- [04.09.2018] Go Pro Fusion Studio 1.2 Privilege Escalation
- [17.07.2018] Microhard Systems 3G/4G Cellular Ethernet and Serial Gateway Backdoor Jailbreak
- [17.07.2018] Microhard Systems 3G/4G Cellular Ethernet and Serial Gateway Arbitrary File Attacks
- [17.07.2018] Microhard Systems 3G/4G Cellular Ethernet and Serial Gateway Configuration Download
- [17.07.2018] Microhard Systems 3G/4G Cellular Ethernet and Serial Gateway Open Redirect
- [17.07.2018] Microhard Systems 3G/4G Cellular Ethernet and Serial Gateway Hidden Features
- [17.07.2018] Microhard Systems 3G/4G Cellular Ethernet and Serial Gateway Service Control DoS
- [17.07.2018] Microhard Systems 3G/4G Cellular Ethernet and Serial Gateway Default Credentials
- [17.07.2018] Microhard Systems 3G/4G Cellular Ethernet and Serial Gateway Remote Root Exploit
- [17.07.2018] Microhard Systems 3G/4G Cellular Ethernet and Serial Gateway CSRF Vulnerabilities
- [17.07.2018] Microhard Systems 3G/4G Cellular Ethernet and Serial Gateway XSS Vulnerabilities
- [24.06.2018] Ecessa ShieldLink SL175EHQ 10.7.4 CSRF Add Superuser Exploit
- [24.06.2018] Ecessa WANWorx WVR-30 10.7.4 CSRF Add Superuser Exploit
- [24.06.2018] Ecessa Edge EV150 10.7.4 CSRF Add Superuser Exploit
- [10.06.2018] Rockwell Automation RSLinx Classic and FactoryTalk Linx Gateway Privilege Escalation
- [05.06.2018] Sint Wind PI v01.26.19 Authentication Bypass
- [29.05.2018] GNU Barcode 0.99 Memory Leak
- [29.05.2018] GNU Barcode 0.99 Buffer Overflow
- [21.05.2018] Epic Games Fortnite 4.2-CL-4072250 Insecure File Permissions
- [21.05.2018] Epic Games Launcher 7.9.4-4058369 Insecure File Permissions
- [21.05.2018] Teradek Slice 7.3.15 CSRF Change Password Exploit
- [21.05.2018] Teradek Slice 7.3.15 (snapshot.cgi) Stream Disclosure
- [21.05.2018] Teradek T-RAX 7.3.2 (snapshot.cgi) Stream Disclosure
- [21.05.2018] Teradek Cube 7.3.6 CSRF Change Password Exploit
- [21.05.2018] Teradek Cube 7.3.6 (snapshot.cgi) Stream Disclosure
- [21.05.2018] Teradek VidiU Pro 3.0.3 (snapshot.cgi) Stream Disclosure
- [21.05.2018] Teradek VidiU Pro 3.0.3 SSRF Vulnerability
- [21.05.2018] Teradek VidiU Pro 3.0.3 CSRF Change Password Exploit
- [07.04.2018] KYOCERA Multi-Set Template Editor 3.4 Out-Of-Band XML External Entity Injection
- [07.04.2018] KYOCERA Net Admin 3.4 CSRF Add Admin Exploit
- [07.04.2018] KYOCERA Net Admin 3.4 Multiple XSS Vulnerabilities
- [02.04.2018] SharpLynx v9.2.3 Insecure File Permissions
- [31.03.2018] VideoFlow Digital Video Protection DVP 10 Authenticated Root Remote Code Execution
- [31.03.2018] VideoFlow Digital Video Protection DVP 10 Authenticated Directory Traversal
- [10.03.2018] Prisma Industriale Checkweigher PrismaWEB 1.21 Authentication Bypass
- [11.02.2018] LogicalDOC Enterprise 7.7.4 Post-Auth Command Execution Via Binary Path Manipulation
- [11.02.2018] LogicalDOC Enterprise 7.7.4 Username Enumeration Weakness
- [11.02.2018] LogicalDOC Enterprise 7.7.4 Multiple Directory Traversal Vulnerabilities
- [11.02.2018] LogicalDOC Enterprise 7.7.4 Reflected Cross-Site Scripting Vulnerabilities
- [22.01.2018] NEC Univerge SV9100/SV8100 WebPro 10.0 Remote Configuration Download

## - 2017 -

- [27.12.2017] Xerox DC260 EFI Fiery Controller Webtools 2.0 Arbitrary File Disclosure
- [27.12.2017] Telesquare SKT LTE Router SDT-CS3B1 WebDAV HTTP Methods Arbitrary File Events
- [27.12.2017] Telesquare SKT LTE Router SDT-CS3B1 Insecure Direct Object Reference Info Leak
- [27.12.2017] Telesquare SKT LTE Router SDT-CS3B1 Remote Reboot Denial Of Service
- [27.12.2017] Telesquare SKT LTE Router SDT-CS3B1 CSRF System Command Execution
- [27.12.2017] Easy!Appointments v1.2.1 Multiple Stored XSS Vulnerabilities
- [24.12.2017] NS International Train Tickets v7.31.4 Reflected XSS Vulnerability
- [15.11.2017] Allworx Server Manager Multiple Cross-Site Scripting Vulnerabilities
- [23.10.2017] Mikogo 5.4.1.160608 Local Credentials Disclosure
- [25.09.2017] FLIR Systems FLIR Thermal Camera PT-Series (PT-334 200562) Remote Root Exploit
- [25.09.2017] FLIR Systems FLIR Thermal Camera FC-S/PT Authenticated OS Command Injection
- [25.09.2017] FLIR Systems FLIR Thermal Camera F/FC/PT/D Hard-Coded SSH Credentials
- [25.09.2017] FLIR Systems FLIR Thermal Camera F/FC/PT/D Stream Disclosure
- [25.09.2017] FLIR Systems FLIR Thermal Camera F/FC/PT/D Multiple Information Disclosures
- [29.08.2017] NethServer 7.3.1611 (create.json) CSRF Create User And Enable SSH Access
- [29.08.2017] NethServer 7.3.1611 (Upload.json) CSRF Script Insertion Vulnerability
- [22.08.2017] Automated Logic WebCTRL 6.5 Unrestricted File Upload Remote Code Execution
- [22.08.2017] Automated Logic WebCTRL 6.1 Path Traversal Arbitrary File Write
- [22.08.2017] Automated Logic WebCTRL 6.5 Insecure File Permissions Privilege Escalation
- [09.08.2017] DALIM SOFTWARE ES Core 5.0 build 7184.1 Server-Side Request Forgery
- [09.08.2017] DALIM SOFTWARE ES Core 5.0 build 7184.1 Multiple Remote File Disclosures
- [09.08.2017] DALIM SOFTWARE ES Core 5.0 build 7184.1 Multiple Stored XSS And CSRF Vulnerabilities
- [09.08.2017] DALIM SOFTWARE ES Core 5.0 build 7184.1 User Enumeration Weakness
- [12.07.2017] Dasan Networks GPON ONT WiFi Router H64X Series System Config Download
- [12.07.2017] Dasan Networks GPON ONT WiFi Router H64X Series Privilege Escalation
- [12.07.2017] Dasan Networks GPON ONT WiFi Router H64X Series Cross-Site Request Forgery
- [12.07.2017] Dasan Networks GPON ONT WiFi Router H64X Series Authentication Bypass



- [\[10.07.2017\] Schneider Electric Pelco VideoXpert Missing Encryption Of Sensitive Information](#)
- [\[10.07.2017\] Schneider Electric Pelco VideoXpert Core Admin Portal Directory Traversal](#)
- [\[10.07.2017\] Schneider Electric Pelco VideoXpert Privilege Escalations](#)
- [\[10.07.2017\] Schneider Electric Pelco Sarix/Spectra Cameras Root Remote Code Execution](#)
- [\[10.07.2017\] Schneider Electric Pelco Sarix/Spectra Cameras CSRF Enable SSH Root Access](#)
- [\[10.07.2017\] Schneider Electric Pelco Sarix/Spectra Cameras Multiple XSS Vulnerabilities](#)
- [\[21.06.2017\] SimpleRisk v20170416-001 Reflected XSS Vulnerabilities](#)
- [\[04.06.2017\] EnGenius EnShare IoT Gigabit Cloud Service 1.4.11 Root Remote Code Execution](#)
- [\[30.05.2017\] OV3 Online Administration 3.0 Multiple Unauthenticated SQL Injection Vulnerabilities](#)
- [\[30.05.2017\] OV3 Online Administration 3.0 Authenticated Code Execution](#)
- [\[30.05.2017\] OV3 Online Administration 3.0 Parameter Traversal Arbitrary File Access PoC Exploit](#)
- [\[28.05.2017\] CERIO 11nbg 2.4Ghz High Power Wireless Router \(pekcmd\) Rootshell Backdoors](#)
- [\[03.05.2017\] Serviio PRO 1.8 DLNA Media Streaming Server REST API Arbitrary Code Execution](#)
- [\[03.05.2017\] Serviio PRO 1.8 DLNA Media Streaming Server REST API Arbitrary Password Change](#)
- [\[03.05.2017\] Serviio PRO 1.8 DLNA Media Streaming Server \(mediabrowser\) DOM Based XSS](#)
- [\[03.05.2017\] Serviio PRO 1.8 DLNA Media Streaming Server Local Privilege Escalation](#)
- [\[03.05.2017\] Serviio PRO 1.8 DLNA Media Streaming Server REST API Information Disclosure](#)
- [\[30.04.2017\] Emby MediaServer 3.2.5 Directory Traversal File Disclosure Vulnerability](#)
- [\[30.04.2017\] Emby MediaServer 3.2.5 Reflected XSS Vulnerability](#)
- [\[30.04.2017\] Emby MediaServer 3.2.5 Password Reset Vulnerability](#)
- [\[30.04.2017\] Emby MediaServer 3.2.5 Boolean-based Blind SQL Injection Vulnerability](#)
- [\[26.03.2017\] Farmer's Fridge Kiosk 2.0.0 Unprotected Event Log Information Disclosure](#)
- [\[12.02.2017\] Cimetrix BACnet Explorer 4.0 XXE Vulnerability](#)
- [\[12.02.2017\] Cimetrix BACstac Routing Service 6.2f Local Privilege Escalation](#)
- [\[11.02.2017\] SonicDICON PACS 2.3.2 Remote Vertical Privilege Escalation Exploit](#)
- [\[11.02.2017\] SonicDICON PACS 2.3.2 CSRF Add Admin Exploit](#)
- [\[11.02.2017\] SonicDICON PACS 2.3.2 Multiple Stored Cross-Site Scripting Vulnerabilities](#)
- [\[29.01.2017\] TrueConf Server v4.3.7 Multiple Remote Web Vulnerabilities](#)

## - 2016 -

- [\[29.12.2016\] Dell SonicWALL Secure Mobile Access SMA 8.1 XSS And WAF CSRF](#)
- [\[29.12.2016\] Dell SonicWALL Network Security Appliance NSA 6600 Reflected XSS](#)
- [\[29.12.2016\] Dell SonicWALL Global Management System GMS 8.1 Adobe Flex SOP Bypass](#)
- [\[29.12.2016\] Dell SonicWALL Global Management System GMS 8.1 XSS Vulnerabilities](#)
- [\[29.12.2016\] Dell SonicWALL Global Management System GMS 8.1 Blind SQL Injection](#)
- [\[16.12.2016\] Horos 2.1.0 Web Portal Remote Information Disclosure Exploit](#)
- [\[16.12.2016\] Horos 2.1.0 DICOM Medical Image Viewer Remote Memory Overflow Vulnerability](#)
- [\[16.12.2016\] Horos 2.1.0 Web Portal DOM Based XSS](#)
- [\[16.12.2016\] DCMTK storescp DICOM storage \(C-STORE\) SCP Remote Stack Buffer Overflow](#)
- [\[16.12.2016\] ConQuest DICOM Server 1.4.17d Remote Stack Buffer Overflow RCE](#)
- [\[16.12.2016\] OsiriX DICOM Viewer 8.0.1 \(dulpase.cc\) Remote Memory Corruption Vulnerability](#)
- [\[16.12.2016\] OsiriX Web Portal 8.0.1 DOM Based XSS](#)
- [\[16.12.2016\] Orthanc DICOM Server 1.1.0 Remote Memory Corruption Vulnerability](#)
- [\[16.12.2016\] Orthanc DICOM Server 1.1.0 Unquoted Service Path Privilege Escalation](#)
- [\[12.12.2016\] Serva 3.0.0 HTTP Server Module Remote Denial of Service Exploit](#)
- [\[30.11.2016\] X5 Webserver 5.0 Remote Denial Of Service Exploit](#)
- [\[29.11.2016\] Peplink NGxxx/LCxxx VPN-Firewall Open Redirect Vulnerability](#)
- [\[28.10.2016\] InfraPower PPS-02-S Q213V1 Cross-Site Request Forgery](#)
- [\[28.10.2016\] InfraPower PPS-02-S Q213V1 Authentication Bypass Vulnerability](#)
- [\[28.10.2016\] InfraPower PPS-02-S Q213V1 Insecure Direct Object Reference Authorization Bypass](#)
- [\[28.10.2016\] InfraPower PPS-02-S Q213V1 Unauthenticated Remote Root Command Execution](#)
- [\[28.10.2016\] InfraPower PPS-02-S Q213V1 Hard-coded Credentials Remote Root Access](#)
- [\[28.10.2016\] InfraPower PPS-02-S Q213V1 Local File Disclosure Vulnerability](#)
- [\[28.10.2016\] InfraPower PPS-02-S Q213V1 Multiple XSS Vulnerabilities](#)
- [\[31.08.2016\] ZKTeco ZKAccess Security System 5.3.1 Stored XSS Vulnerability](#)
- [\[31.08.2016\] ZKTeco ZKBioSecurity 3.0 \(visLogin.jsp\) Local Authorization Bypass](#)
- [\[31.08.2016\] ZKTeco ZKBioSecurity 3.0 User Enumeration Weakness](#)
- [\[31.08.2016\] ZKTeco ZKBioSecurity 3.0 File Path Manipulation Vulnerability](#)
- [\[31.08.2016\] ZKTeco ZKBioSecurity 3.0 CSRF Add Superadmin Exploit](#)
- [\[30.08.2016\] ZKTeco ZKBioSecurity 3.0 Multiple XSS Vulnerabilities](#)
- [\[30.08.2016\] ZKTeco ZKBioSecurity 3.0 Hardcoded Credentials Remote SYSTEM Code Execution](#)
- [\[30.08.2016\] ZKTeco ZKAccess Professional 3.5.3 Insecure File Permissions](#)
- [\[30.08.2016\] ZKTeco ZKTime.Net 3.0.1.6 Insecure File Permissions](#)
- [\[21.08.2016\] Newtec Satellite Modem MDM6000 2.2.5 Cross-Site Scripting Vulnerability](#)
- [\[21.08.2016\] Sakai 10.7 Multiple Vulnerabilities](#)
- [\[10.08.2016\] EyeLock nano NXT 3.5 Remote Root Exploit](#)
- [\[10.08.2016\] EyeLock nano NXT 3.5 Local File Disclosure Vulnerability](#)
- [\[10.08.2016\] EyeLock Myris 3.3.2 SDK Service Unquoted Service Path Privilege Escalation](#)
- [\[06.08.2016\] NUUO Backdoor \(strong\\_user.php\) Remote Shell Access](#)
- [\[06.08.2016\] NUUO Arbitrary File Deletion Vulnerability](#)
- [\[06.08.2016\] NUUO NVRmini 2 NE-4160 ShellShock Remote Code Execution](#)
- [\[06.08.2016\] NUUO Multiple OS Command Injection Vulnerabilities](#)
- [\[06.08.2016\] NUUO Local File Disclosure Vulnerability](#)
- [\[06.08.2016\] NUUO CSRF Add Admin Exploit](#)
- [\[06.08.2016\] NUUO Remote Root Exploit](#)
- [\[26.07.2016\] Iris ID IrisAccess iCAM4000/iCAM7000 Hardcoded Credentials Remote Shell Access](#)
- [\[26.07.2016\] Iris ID IrisAccess ICU 7000-2 Remote Root Command Execution](#)
- [\[26.07.2016\] Iris ID IrisAccess ICU 7000-2 Multiple XSS and CSRF Vulnerabilities](#)
- [\[22.07.2016\] Rapid7 AppSpider 6.12 Web Application Vulnerability Scanner Elevation Of Privilege](#)
- [\[19.07.2016\] Wowza Streaming Engine 4.5.0 Multiple Cross-Site Scripting Vulnerabilities](#)
- [\[19.07.2016\] Wowza Streaming Engine 4.5.0 Cleartext Storage Of Sensitive Information](#)
- [\[19.07.2016\] Wowza Streaming Engine 4.5.0 CSRF Add Advanced Admin Exploit](#)
- [\[19.07.2016\] Wowza Streaming Engine 4.5.0 Remote Privilege Escalation Exploit](#)
- [\[19.07.2016\] Wowza Streaming Engine 4.5.0 Local Privilege Escalation](#)
- [\[08.07.2016\] CyberPower Systems PowerPanel 3.1.2 XXE Out-Of-Band Data Retrieval](#)
- [\[05.07.2016\] AWBS v2.9.6 Multiple Remote Vulnerabilities](#)
- [\[01.07.2016\] eCardMAX 10.5 Multiple Vulnerabilities](#)
- [\[01.07.2016\] XpoLog Center V6 CSRF Remote Command Execution](#)
- [\[01.07.2016\] XpoLog Center V6 Multiple Remote Vulnerabilities](#)
- [\[25.06.2016\] Option CloudGate Insecure Direct Object References Authorization Bypass](#)
- [\[24.06.2016\] iBilling v3.7.0 Multiple Stored and Reflected Cross-Site Scripting Vulnerabilities](#)
- [\[20.06.2016\] ACROS Security Opatch \(OPatchServicex64.exe\) Unquoted Service Path EoP](#)
- [\[16.06.2016\] Gemalto Sentinel License Manager 18.0.1 Directory Traversal Vulnerability](#)

- [14.06.2016] Hyperoptic (Tilgin) Router HG23xx Multiple XSS And CSRF Vulnerabilities
- [30.05.2016] FlatPress 1.0.3 CSRF Arbitrary File Upload
- [26.05.2016] Micro Focus Rumba+ v9.4 Multiple Stack Buffer Overflow Vulnerabilities
- [25.05.2016] EduSec 4.2.5 Multiple SQL Injection Vulnerabilities
- [25.05.2016] Real Estate Portal v4.1 Remote Code Execution and Persistent XSS Vulnerabilities
- [22.05.2016] Operation Technology ETAP 14.1.0 Multiple Stack Buffer Overrun Vulnerabilities
- [22.05.2016] Operation Technology ETAP 14.1.0 Local Privilege Escalation
- [22.05.2016] JobScript Open Redirection And Arbitrary Code Execution Vulnerability
- [08.05.2016] Certec EDV atvise SCADA server 2.5.9 Privilege Escalation Vulnerability
- [06.05.2016] Ajaxel CMS 8.0 Multiple Vulnerabilities
- [06.05.2016] ZeewaysCMS Multiple Vulnerabilities
- [23.04.2016] NationBuilder Multiple Stored XSS Vulnerabilities
- [13.04.2016] OpenWGA Developer Studio 3.1.0 OpenFileDialog Arbitrary Code Execution
- [13.04.2016] OpenWGA Content Manager 7.1.9 User-Agent HTTP Header XSS Vulnerability
- [08.04.2016] Hikvision Digital Video Recorder Cross-Site Request Forgery
- [05.04.2016] Asbru Web Content Management System v9.2.7 Multiple Vulnerabilities
- [04.04.2016] Sophos Cyberoam NG Series Multiple Cross-Site Scripting Vulnerabilities
- [30.03.2016] MOBOTIX Video Security Cameras CSRF Add Admin Exploit
- [15.03.2016] Netwrix Auditor 7.1.322.0 ActiveX (sourceFile) Stack Buffer Overflow Vulnerability
- [29.02.2016] Crouzet em4 soft 1.1.04 and M3 soft 3.1.2.0 Insecure File Permissions
- [29.02.2016] Crouzet em4 soft 1.1.04 Integer Division By Zero
- [26.02.2016] Infor CRM 8.2.0.1136 Multiple HTML Script Injection Vulnerabilities
- [23.02.2016] ManageEngine Firewall Analyzer 8.5 SP-5.0 Multiple XSS Vulnerabilities
- [16.02.2016] Inductive Automation Ignition 7.8.1 Remote Leakage Of Shared Buffers
- [14.02.2016] Delta Industrial Automation DCISoft 1.12.09 Stack Buffer Overflow Exploit
- [10.02.2016] Wieland wieplan 4.1 Document Parsing Java Code Execution Using XMLDecoder
- [02.02.2016] Baumer VeriSens Application Suite 2.6.2 Buffer Overflow Vulnerability
- [01.02.2016] Autonics DAQMaster 1.7.3 DQP Parsing Buffer Overflow Code Execution
- [30.01.2016] Hippo CMS 10.1 XML External Entity Information Disclosure Vulnerability
- [30.01.2016] Hippo CMS 10.1 Stored Cross-Site Scripting Vulnerability
- [28.01.2016] HP Client Security Manager 8.3.4 Cross-Site Scripting Vulnerability
- [28.01.2016] iScripts EasyCreate 3.0 Multiple Vulnerabilities
- [28.01.2016] iScripts EasyCreate 3.0 Remote Code Execution Exploit
- [19.01.2016] BlueControl 3.5 SR5 Insecure Library Loading Arbitrary Code Execution
- [17.01.2016] Art Systems FluidDraw P5/S5 5.3n Binary Planting Arbitrary Code Execution
- [16.01.2016] WEG SuperDrive G2 v12.0.0 Insecure File Permissions
- [14.01.2016] dbaudio R1 v2.14.4 DNS-SD Service Unquoted Service Path Privilege Escalation
- [13.01.2016] Manage Engine Applications Manager 12 Multiple Vulnerabilities
- [13.01.2016] Applications Manager 12.5 Arbitrary Command Execution Exploit

## - 2015 -

- [08.12.2015] dotCMS 3.2.4 Multiple Vulnerabilities
- [07.12.2015] OpenMRS 2.3 (1.11.4) XML External Entity (XXE) Processing PoC Exploit
- [07.12.2015] OpenMRS 2.3 (1.11.4) Expression Language Injection Vulnerability
- [07.12.2015] OpenMRS 2.3 (1.11.4) Multiple Cross-Site Scripting Vulnerabilities
- [07.12.2015] OpenMRS 2.3 (1.11.4) Local File Disclosure Vulnerability
- [07.12.2015] GEOVAP Reliance 4 Control Server Unquoted Service Path Elevation Of Privilege
- [06.12.2015] iniNet SpiderControl SCADA Web Server Service 2.02 Insecure File Permissions
- [06.12.2015] iniNet SpiderControl PLC Editor Simatic 6.30.04 Insecure File Permissions
- [06.12.2015] iniNet SpiderControl SCADA Editor 6.30.01 Insecure File Permissions
- [05.12.2015] Circutor PowerStudio SCADA 4.0.5 Unquoted Service Path Elevation Of Privilege
- [17.11.2015] Zenario CMS 7.0.7c Remote Code Execution Vulnerability
- [15.11.2015] TECO JN5 L510-DriveLink 1.482 SEH Overwrite Buffer Overflow Exploit
- [15.11.2015] TECO AP-PCLINK 1.094 TPC File Handling Buffer Overflow Vulnerability
- [15.11.2015] TECO TP3-PCLINK 2.1 TPC File Handling Buffer Overflow Vulnerability
- [15.11.2015] TECO SG2 FBD Client 3.51 SEH Overwrite Buffer Overflow Vulnerability
- [15.11.2015] TECO SG2 LAD Client 3.51 SEH Overwrite Buffer Overflow Exploit
- [11.11.2015] R-Scripts VRS 7R Multiple Stored XSS And CSRF Vulnerabilities
- [31.10.2015] actiTIME 2015.2 Multiple Vulnerabilities
- [22.10.2015] Realtyna RPL 8.9.2 Joomla Extension Multiple SQL Injection Vulnerabilities
- [22.10.2015] Realtyna RPL 8.9.2 Joomla Extension Persistent XSS And CSRF Vulnerabilities
- [19.10.2015] RealtyScript v4.0.2 Multiple Time-based Blind SQL Injection Vulnerabilities
- [19.10.2015] RealtyScript v4.0.2 Multiple CSRF And Persistent XSS Vulnerabilities
- [11.10.2015] Dream CMS 2.3.0 CSRF Add Extension And File Upload PHP Code Execution
- [07.10.2015] Kallithea 0.2.9 (came\_from) HTTP Response Splitting Vulnerability
- [26.09.2015] Centreon 2.6.1 Stored Cross-Site Scripting Vulnerability
- [26.09.2015] Centreon 2.6.1 Command Injection Vulnerability
- [26.09.2015] Centreon 2.6.1 Unrestricted File Upload Vulnerability
- [26.09.2015] Centreon 2.6.1 CSRF Add Admin Exploit
- [26.09.2015] Mango Automation 2.6.0 CSRF File Upload And Arbitrary JSP Code Execution
- [26.09.2015] Mango Automation 2.6.0 CSRF Arbitrary Command Execution Exploit
- [26.09.2015] Mango Automation 2.6.0 Unprotected Debug Log View Vulnerability
- [26.09.2015] Mango Automation 2.6.0 CSRF Arbitrary SQL Query Execution
- [26.09.2015] Mango Automation 2.6.0 CSRF Add Admin Exploit
- [26.09.2015] Mango Automation 2.6.0 Remote XSS POST Injection Vulnerability
- [26.09.2015] Mango Automation 2.6.0 User Enumeration Weakness
- [14.09.2015] TP-Link NC200/NC220 Cloud Camera 300Mbps Wi-Fi Hard-Coded Credentials
- [19.08.2015] up.time 7.5.0 Upload And Execute File Exploit
- [19.08.2015] up.time 7.5.0 Arbitrary File Disclose And Delete Exploit
- [19.08.2015] up.time 7.5.0 XSS And CSRF Add Admin Exploit
- [19.08.2015] up.time 7.5.0 Superadmin Privilege Escalation Exploit
- [04.08.2015] Microweber v1.0.3 File Upload Filter Bypass Remote PHP Code Execution
- [04.08.2015] Microweber v1.0.3 Stored XSS And CSRF Add Admin Exploit
- [13.07.2015] ArticleFR 3.0.6 CSRF Add Admin Exploit
- [13.07.2015] ArticleFR 3.0.6 Multiple Script Injection Vulnerabilities
- [13.06.2015] Cisco AnyConnect Secure Mobility Client Remote Command Execution
- [06.06.2015] Netlux Antivirus 1.0.1.8 Session Manager Service Privilege Escalation
- [28.05.2015] IBM Cognos Business Intelligence Developer 10.2.1 (backURL) Open Redirect
- [24.05.2015] Acoustica Pianissimo 1.0 Build 12 (Registration ID) Buffer Overflow PoC
- [14.04.2015] WordPress MiwoFTP Plugin 1.0.5 CSRF Arbitrary File Creation Exploit (RCE)
- [14.04.2015] WordPress MiwoFTP Plugin 1.0.5 Multiple CSRF XSS Vulnerabilities
- [14.04.2015] WordPress MiwoFTP Plugin 1.0.5 CSRF Arbitrary File Deletion Exploit
- [07.04.2015] Balero CMS v0.7.2 Multiple JS/HTML Injection Vulnerabilities

- [07.04.2015] Balero CMS v0.7.2 Multiple Blind SQL Injection Vulnerabilities
- [16.03.2015] Spybot Search & Destroy 1.6.2 Security Center Service Privilege Escalation
- [16.03.2015] Moodle 2.5.9/2.6.8/2.7.5/2.8.3 Block Title Handler Cross-Site Scripting
- [14.03.2015] Foxit Reader 7.0.6.1126 Unquoted Service Path Elevation Of Privilege
- [10.03.2015] GeniXCMS v0.0.1 CSRF Add Admin Exploit
- [10.03.2015] GeniXCMS v0.0.1 Persistent Script Insertion Vulnerability
- [10.03.2015] GeniXCMS v0.0.1 Remote Unauthenticated SQL Injection Exploit
- [26.02.2015] Electronic Arts Origin Client 9.5.5 Multiple Privilege Escalation Vulnerabilities
- [25.02.2015] Ubisoft Uplay 5.0 Insecure File Permissions Local Privilege Escalation
- [25.02.2015] Alienware Command Center 2.8.8.0 Local Privilege Escalation
- [24.02.2015] Realtek 11n Wireless LAN Utility Privilege Escalation
- [09.02.2015] u5CMS 3.9.3 Multiple Open Redirect Vulnerabilities
- [09.02.2015] u5CMS 3.9.3 (deletefile.php) Arbitrary File Deletion Vulnerability
- [09.02.2015] u5CMS 3.9.3 Multiple SQL Injection Vulnerabilities
- [09.02.2015] u5CMS 3.9.3 (thumb.php) Local File Inclusion Vulnerability
- [09.02.2015] u5CMS 3.9.3 Multiple Stored And Reflected XSS Vulnerabilities
- [12.01.2015] Gecko CMS 2.3 Multiple Vulnerabilities
- [07.01.2015] Zurmo CRM 2.8.5 Multiple Reflected Cross-Site Scripting Vulnerabilities
- [05.01.2015] AdaptCMS 3.0.3 Remote Command Execution Exploit
- [05.01.2015] AdaptCMS 3.0.3 HTTP Referer Header Field Open Redirect Vulnerability
- [05.01.2015] AdaptCMS 3.0.3 Multiple Persistent XSS Vulnerabilities

## - 2014 -

- [23.12.2014] BitRaider Streaming Client 1.3.3.4098 Local Privilege Escalation Vulnerability
- [14.12.2014] Soitec SmartEnergy 1.4 SCADA Login SQL Injection Authentication Bypass Exploit
- [08.12.2014] IceHrm <=7.1 Multiple Vulnerabilities
- [02.12.2014] IPUX Cube Type CS303C IP Camera (UltraMJCmX.ocx) ActiveX Stack Buffer Overflow
- [02.12.2014] IPUX CL5452/CL5132 IP Camera (UltraSVCmX.ocx) ActiveX Stack Buffer Overflow
- [02.12.2014] IPUX CS7522/CS2330/CS2030 IP Camera (UltraHVCmX.ocx) ActiveX Stack BoF
- [25.11.2014] TRENDnet SecurView Wireless Network Camera TV-IP422WN (UltraCamX.ocx) Stack BoF
- [22.11.2014] TP-Link TL-WR740N Wireless Router MitM httpd Denial Of Service
- [21.11.2014] Privacyware Privatefirewall 7.0 Unquoted Service Path Privilege Escalation
- [21.11.2014] Netgear Wireless Router WNR500 Parameter Traversal Arbitrary File Access Exploit
- [20.11.2014] Zenario CMS 7.0.2d Reflected XSS and Open Redirect Vulnerabilities
- [18.11.2014] Snowfox CMS v1.0 (rd param) Open Redirect Vulnerability
- [18.11.2014] Snowfox CMS v1.0 CSRF Add Admin Exploit
- [12.11.2014] CorelDRAW X7 CDR File (CdrTxt.dll) Off-By-One Stack Corruption Vulnerability
- [25.10.2014] CBN CH6640E/CG6640E Wireless Gateway Series Multiple Vulnerabilities
- [12.10.2014] Croogo 2.0.0 Arbitrary PHP Code Execution Exploit
- [12.10.2014] Croogo 2.0.0 Multiple Stored XSS Vulnerabilities
- [09.10.2014] Telefonica O2 Connection Manager 8.7 Service Trusted Path Privilege Escalation
- [09.10.2014] Telefonica O2 Connection Manager 3.4 Local Privilege Escalation Vulnerability
- [30.07.2014] SkaDate Lite 2.0 Remote Code Execution Exploit
- [30.07.2014] SkaDate Lite 2.0 Multiple XSRF And Persistent XSS Vulnerabilities
- [28.07.2014] Oxwall 1.7.0 Remote Code Execution Exploit
- [28.07.2014] Oxwall 1.7.0 Multiple CSRF And HTML Injection Vulnerabilities
- [24.07.2014] Omeka 2.2.1 Remote Code Execution Exploit
- [17.07.2014] Omeka 2.2 CSRF And Stored XSS Vulnerability
- [11.07.2014] OpenVPN Private Tunnel Core Service Unquoted Service Path Elevation Of Privilege
- [03.07.2014] Ubisoft Uplay 4.6 Insecure File Permissions Local Privilege Escalation
- [30.06.2014] Baidu Spark Browser v26.5.9999.3511 Remote Stack Overflow Vulnerability (DoS)
- [21.06.2014] Lunar CMS 3.3 Unauthenticated Remote Command Execution Exploit
- [21.06.2014] Lunar CMS 3.3 CSRF And Stored XSS Vulnerability
- [17.06.2014] Ubisoft Rayman Legends v1.2.103716 Remote Stack Buffer Overflow Vulnerability
- [09.06.2014] ZeroCMS 1.0 (article\_id) SQL Injection Vulnerability
- [28.04.2014] NULL NUKE CMS v2.2 Multiple Vulnerabilities
- [24.04.2014] cFos Personal Net v3.09 Remote Heap Memory Corruption Denial of Service
- [03.04.2014] MA Lighting Technology grandMA onPC v6.808 Remote Denial of Service Exploit
- [25.03.2014] Cart Engine 3.0.0 Remote Code Execution
- [25.03.2014] Cart Engine 3.0.0 (task.php) Local File Inclusion Vulnerability
- [25.03.2014] Cart Engine 3.0.0 Database Backup Disclosure Exploit
- [25.03.2014] Kemana Directory 1.5.6 kemana\_admin\_passwd Cookie User Password Hash Disclosure
- [25.03.2014] Kemana Directory 1.5.6 Remote Code Execution
- [25.03.2014] Kemana Directory 1.5.6 (run param) Local File Inclusion Vulnerability
- [25.03.2014] Kemana Directory 1.5.6 Database Backup Disclosure Exploit
- [25.03.2014] Kemana Directory 1.5.6 (qvc\_init()) Cookie Poisoning CAPTCHA Bypass Exploit
- [25.03.2014] qEngine CMS 6.0.0 Remote Code Execution
- [25.03.2014] qEngine CMS 6.0.0 (task.php) Local File Inclusion Vulnerability
- [25.03.2014] qEngine CMS 6.0.0 Database Backup Disclosure Exploit
- [10.03.2014] Huawei Technologies eSpace Meeting Service 1.0.0.23 Local Privilege Escalation
- [28.02.2014] couponPHP CMS 1.0 Multiple Stored XSS and SQL Injection Vulnerabilities
- [20.02.2014] Stark CRM v1.0 Multiple Script Injection And Session Riding Vulnerabilities
- [06.02.2014] Asseco SEE iBank FX Client <= 2.0.9.3 Local Privilege Escalation Vulnerability
- [29.01.2014] NCH Software Inventoria 3.45 (id param) Reflected Cross-Site Scripting Vulnerability
- [21.01.2014] NCH Software Express Burn Plus 4.68 EBP Project File Handling Buffer Overflow PoC
- [02.01.2014] ACE Stream Media 2.1 (acestream://) Format String Exploit PoC

## - 2013 -

- [19.12.2013] Huawei Technologies du Mobile Broadband 16.0 Local Privilege Escalation
- [06.12.2013] BoxBilling 3.6.11 (mod\_notification) Stored Cross-Site Scripting Vulnerability
- [28.11.2013] Ametys CMS 3.5.2 (lang parameter) XPath Injection Vulnerability
- [23.11.2013] LimeSurvey v2.00+ (build 131107) Script Insertion And SQL Injection Vulnerability
- [03.11.2013] Practico 13.9 Multiple Vulnerabilities
- [01.11.2013] ImpressPages CMS v3.6 manage() Function Remote Code Execution Exploit
- [31.10.2013] ImpressPages CMS v3.6 Remote Arbitrary File Deletion Vulnerability
- [31.10.2013] ImpressPages CMS v3.6 Multiple XSS/SQLi Vulnerabilities
- [18.10.2013] Wordpress WooCommerce Plugin 2.0.17 Cross-Site Scripting Vulnerability
- [18.09.2013] TeraCopy 2.3 (default.mo) Language File Integer Overflow Vulnerability

- [22.08.2013] Ovidentia 7.9.4 Multiple Remote Vulnerabilities
- [11.08.2013] Gnew v2013.1 Multiple XSS And SQL Injection Vulnerabilities
- [07.08.2013] MyBB 1.6.10 'url' Parameter Arbitrary Site Redirection Vulnerability
- [06.08.2013] Atlassian JIRA v6.0.3 Arbitrary HTML/Script Execution Vulnerability
- [29.07.2013] FluxBB 1.5.3 Multiple Remote Vulnerabilities
- [24.07.2013] Windu CMS 2.2 CSRF Add Admin Exploit
- [24.07.2013] Windu CMS 2.2 Multiple Persistent Cross-Site Scripting Vulnerabilities
- [01.07.2013] Barracuda SSL VPN 680Vx 2.3.3.193 Multiple Script Injection Vulnerabilities
- [19.06.2013] GLPI v0.83.8 Multiple Error-based SQL Injection Vulnerabilities
- [19.06.2013] GLPI v0.83.7 (itemtype) Parameter Traversal Arbitrary File Access Exploit
- [07.06.2013] Resin Application Server 4.0.36 Source Code Disclosure Vulnerability
- [07.06.2013] Resin Application Server 4.0.36 Cross-Site Scripting Vulnerabilities
- [25.05.2013] SAS Integration Technologies Client 9.31\_M1 (SASspk.dll) Stack-based Overflow
- [14.05.2013] Wordpress Newsletter Plugin 3.2.6 (alert) Reflected XSS Vulnerability
- [11.05.2013] Wordpress Securimage-WP Plugin v3.2.4 URI-based XSS Vulnerability
- [10.05.2013] Securimage 3.5 URI-based Cross-Site Scripting Vulnerability
- [14.04.2013] CMSLogik 1.2.1 (upload\_file\_ajax()) Shell Upload Exploit
- [14.04.2013] CMSLogik 1.2.1 (user param) User Enumeration Weakness
- [14.04.2013] CMSLogik 1.2.1 Multiple Persistent XSS Vulnerabilities
- [21.03.2013] TP-Link TL-WR740N Wireless Router Remote Denial Of Service Exploit
- [06.03.2013] Qool CMS v2.0 RC2 XSRF Add Root Exploit
- [06.03.2013] Qool CMS v2.0 RC2 Multiple HTML And JavaScript Injection Vulnerabilities
- [25.02.2013] MTP Poll 1.0 Multiple Remote Script Insertion Vulnerabilities
- [25.02.2013] MTP Guestbook 1.0 Multiple Remote Script Insertion Vulnerabilities
- [25.02.2013] MTP Image Gallery 1.0 (title) Remote Script Insertion Vulnerability
- [21.02.2013] OpenEMR 4.1.1 (site param) Remote XSS Vulnerability
- [19.02.2013] Squirrelcart v3.5.4 (table) Remote Cross-Site Scripting Vulnerability
- [18.02.2013] Piwigo 2.4.6 (install.php) Remote Arbitrary File Read/Delete Vulnerability
- [13.02.2013] OpenEMR 4.1.1 (ofc\_upload\_image.php) Arbitrary File Upload Vulnerability
- [13.02.2013] AbanteCart 1.1.3 (index.php) Multiple Reflected XSS Vulnerabilities
- [20.01.2013] Aloaha Credential Provider Monitor 5.0.226 Local Privilege Escalation Vulnerability
- [13.01.2013] phlyLabs phlyMail Lite 4.03.04 (go param) Open Redirect Vulnerability
- [13.01.2013] phlyLabs phlyMail Lite 4.03.04 Path Disclosure and Stored XSS Vulnerabilities
- [08.01.2013] Joomla Incapsula Component <= 1.4.6\_b Reflected Cross-Site Scripting Vulnerability

## - 2012 -

- [20.12.2012] Sony PC Companion 2.1 (Admin\_RemoveDirectory()) Stack-based Unicode BoF
- [20.12.2012] Sony PC Companion 2.1 (CheckCompatibility()) Stack-based Unicode Buffer Overload
- [20.12.2012] Sony PC Companion 2.1 (Load()) Stack-based Unicode Buffer Overload SEH
- [20.12.2012] Sony PC Companion 2.1 (DownloadURLToFile()) Stack-based Unicode Buffer Overload SEH
- [06.12.2012] NVIDIA Install Application 2.1002.85.551 (NVI2.dll) Unicode Buffer Overflow PoC
- [30.11.2012] Axis Commerce 0.8.7.2 Remote Script Insertion Vulnerabilities
- [28.11.2012] Oracle OpenSSO 8.0 Multiple XSS POST Injection Vulnerabilities
- [26.11.2012] PRADO PHP Framework 3.2.0 Arbitrary File Read Vulnerability
- [26.10.2012] NASA Tri-Agency Climate Education (TrACE) v1.0 SQL Injection Vulnerability
- [26.10.2012] NASA Tri-Agency Climate Education (TrACE) v1.0 Multiple XSS Vulnerabilities
- [04.10.2012] Oracle Identity Management 10g (username) XSS POST Injection Vulnerability
- [25.09.2012] ViArt Shop Enterprise 4.1 Arbitrary Command Execution Vulnerability
- [25.09.2012] ViArt Shop Enterprise 4.1 (post-auth) Multiple Stored XSS Vulnerabilities
- [17.09.2012] Spiceworks 6.0.00993 Multiple Script Injection Vulnerabilities
- [11.09.2012] Subrion CMS 2.2.1 CSRF Add Admin Exploit
- [11.09.2012] Subrion CMS 2.2.1 Multiple Remote XSS POST Injection Vulnerabilities
- [06.09.2012] Cannonbolt Portfolio Manager v1.0 Stored XSS and SQL Injection Vulnerabilities
- [28.08.2012] Express Burn Plus v4.58 EBP Project File Handling Buffer Overflow PoC
- [23.08.2012] xt:Commerce v4.0.15 (products\_name\_de) Script Insertion Vulnerability
- [23.08.2012] Monstra 1.2.1 Multiple HTML Injection Vulnerabilities
- [23.08.2012] KindEditor 4.1.2 (name parameter) Reflected XSS Vulnerability
- [23.08.2012] web@all CMS 2.0 (\_order) SQL Injection Vulnerability
- [23.08.2012] web@all CMS 2.0 Multiple Remote XSS Vulnerabilities
- [23.08.2012] SiNG cms 2.9.0 (email) Remote XSS POST Injection Vulnerability
- [06.08.2012] Zoho BugTracker Multiple Stored XSS Vulnerabilities
- [05.08.2012] PolarisCMS (blog.aspx) Remote URI Based Cross-Site Scripting Vulnerability
- [20.06.2012] IBM System Storage DS Storage Manager Profiler Multiple Vulnerabilities
- [12.06.2012] Apple iTunes 10.6.1.7 M3U Playlist File Walking Heap Buffer Overflow
- [04.06.2012] PyroCMS 2.1.1 CRLF Injection And Stored XSS Vulnerability
- [16.05.2012] Artiphp CMS 5.5.0 Database Backup Disclosure Exploit
- [16.05.2012] Artiphp CMS v5.5.0 Multiple XSS POST Injection Vulnerabilities
- [16.05.2012] backupDB() v1.2.7a (onlyDB) Remote XSS Vulnerability
- [16.05.2012] phpThumb() v1.7.11 (dir & title) Cross-Site Scripting Vulnerability
- [09.05.2012] Andromeda Streaming MP3 Server v1.9.3.6 (s param) Remote XSS Vulnerability
- [02.05.2012] Baby Gekko CMS v1.1.5c Multiple Stored Cross-Site Scripting Vulnerabilities
- [20.04.2012] Anchor CMS v0.6 Multiple Persistent XSS Vulnerabilities
- [11.04.2012] BGS CMS v2.2.1 Multiple Stored Cross-Site Scripting Vulnerabilities
- [03.04.2012] Zend Optimizer 3.3.3 (Windows) Insecure Permissions
- [23.03.2012] Spotify 0.8.2.610 (search func) Memory Exhaustion Exploit
- [21.03.2012] phpList 2.10.17 Remote SQL Injection and XSS Vulnerability
- [20.03.2012] Oreans WinLicense v2.1.8.0 XML File Handling Unspecified Memory Corruption
- [20.03.2012] Oreans Themida v2.1.8.0 TMD File Handling Buffer Overflow Vulnerability
- [10.03.2012] Zend Server 5.6.0 Multiple Remote Script Insertion Vulnerabilities
- [07.03.2012] Promise WebPAM v2.2.0.13 Multiple Remote Vulnerabilities
- [06.03.2012] Fork CMS 3.2.7 Multiple HTML Code Injection Vulnerabilities
- [25.02.2012] webgrind 1.0 (file param) Local File Inclusion Vulnerability
- [17.02.2012] SQL Buddy 1.3.3 (GET/POST) Multiple Remote Cross-Site Scripting Vulnerabilities
- [17.02.2012] webgrind 1.0 (dataFile) Remote Reflected XSS Vulnerability
- [17.02.2012] WampServer <= 2.2c (lang) Remote Cross-Site Scripting Vulnerability
- [08.02.2012] SciTools Understand 2.6 DLL Loading Arbitrary Code Execution
- [07.02.2012] ManageEngine ADManager Plus 5.2 Multiple XSS Vulnerabilities
- [31.01.2012] EdrawSoft Office Viewer Component ActiveX 5.6 (officeviewermmme.ocx) BoF PoC
- [31.01.2012] Mindjet MindManager 2012 v10.0.493 Multiple Remote Vulnerabilities
- [29.01.2012] Tracker Software pdfSaver ActiveX 3.60 (pdfxctrl.dll) Stack Buffer Overflow (SEH)
- [04.01.2012] Limny 3.0.1 (login.php) Remote URI Based Cross-Site Scripting Vulnerability



- 2011 -

- [21.12.2011] Infoproject Biznis Heroj (login.php) Authentication Bypass Vulnerability
- [21.12.2011] Infoproject Biznis Heroj (XSS/SQLi) Multiple Remote Vulnerabilities
- [05.12.2011] SopCast 3.4.7 sop:// URI Handling Remote Stack Buffer Overflow PoC
- [05.12.2011] SopCast 3.4.7 (Diagnose.exe) Improper Permissions
- [01.12.2011] Hero Framework 3.69 Remote Reflected Cross-Site Scripting Vulnerability
- [28.11.2011] Manx cms.xml 1.0.1 (simplexml\_load\_file()) Directory Traversal Vulnerability
- [28.11.2011] Manx cms.xml 1.0.1 Multiple HTTP Response Splitting Vulnerabilities
- [28.11.2011] Manx cms.xml 1.0.1 (ajax\_get\_file\_listing.php) Multiple XSS Vulnerabilities
- [13.11.2011] Hotaru CMS 1.4.2 SITE\_NAME Parameter Stored XSS Vulnerability
- [10.11.2011] Soda PDF Professional 1.2.155 PDF/WWF File Handling Restriction of Service (RoS)
- [08.11.2011] 11in1 CMS v1.0.1 (do.php) CRLF Injection Vulnerability
- [07.11.2011] XAMPP 1.7.7 Multiple URI Based Cross-Site Scripting Vulnerabilities
- [02.11.2011] SetSeed CMS 5.8.20 (loggedInUser) Remote SQL Injection Vulnerability
- [26.10.2011] vtiger CRM 5.2.1 Multiple Remote Cross-Site Scripting Vulnerabilities
- [10.10.2011] Cotonti CMS v0.9.4 Multiple Remote Vulnerabilities
- [04.10.2011] Ashampoo Burning Studio Elements 10.0.9 (.ashprj) Heap Overflow Vulnerability
- [01.10.2011] Adobe Photoshop Elements 8.0 Multiple Arbitrary Code Execution Vulnerabilities
- [19.09.2011] Toko Lite CMS 1.5.2 (edit.php) HTTP Response Splitting Vulnerability
- [19.09.2011] Toko Lite CMS 1.5.2 (EditNavBar.php) Multiple Parameters XSS POST Injection
- [17.09.2011] iGallery Plugin v1.0.0 (dir) Remote Cross-Site Scripting Vulnerability
- [17.09.2011] iManager Plugin v1.2.8 (dir) Remote Cross-Site Scripting Vulnerability
- [17.09.2011] iBrowser Plugin v1.4.1 (dir) Remote Cross-Site Scripting Vulnerability
- [16.09.2011] iManager Plugin v1.2.8 (d) Remote Arbitrary File Deletion Vulnerability
- [16.09.2011] iManager Plugin v1.2.8 (lang) Local File Inclusion Vulnerability
- [16.09.2011] iBrowser Plugin v1.4.1 (lang) Local File Inclusion Vulnerability
- [28.08.2011] Mini FTP Server 1.1 Buffer Corruption Remote Denial Of Service Exploit
- [23.08.2011] ManageEngine ServiceDesk Plus 8.0 Multiple Stored XSS Vulnerabilities
- [14.08.2011] F-Secure BlackLight 2.2.1092 Local Privilege Escalation Vulnerability
- [06.08.2011] ATutor 2.0.2 (lang) HTTP Response Splitting Vulnerability
- [06.08.2011] ATutor 2.0.2 Multiple Remote Vulnerabilities (SQLi/XSS/PD)
- [06.08.2011] AChecker 1.2 Multiple Remote XSS/PD Vulnerabilities
- [06.08.2011] AChecker 1.2 Multiple Error-Based SQL Injection Vulnerabilities
- [06.08.2011] AContent 1.1 (category\_name) Remote Script Insertion Vulnerability
- [06.08.2011] AContent 1.1 Multiple Cross-Site Scripting Vulnerabilities
- [06.08.2011] AContent 1.1 Multiple SQL Injection Vulnerabilities
- [31.07.2011] Digital Scribe 1.5 (register\_form()) Multiple POST XSS Vulnerabilities
- [25.07.2011] Online Grades 3.2.5 Multiple XSS Vulnerabilities
- [14.07.2011] PG eLMS Pro vDEC\_2007\_01 Multiple Blind SQL Injection Vulnerabilities
- [14.07.2011] PG eLMS Pro vDEC\_2007\_01 (contact\_us.php) Multiple POST XSS Vulnerabilities
- [13.07.2011] TCEXam <=11.2.011 Multiple SQL Injection Vulnerabilities
- [13.07.2011] TCEXam <=11.2.011 Multiple Cross-Site Scripting Vulnerabilities
- [10.07.2011] Tugux CMS 1.2 (pid) Remote Arbitrary File Deletion Vulnerability
- [06.07.2011] ESTsoft ALPlayer 2.0 ASX Playlist File Handling Buffer Overflow Vulnerability
- [29.06.2011] Valve Steam Client Application v1559/1559 Local Privilege Escalation
- [23.06.2011] NetServe Web Server v1.0.58 Multiple Remote Vulnerabilities
- [21.06.2011] Sitemagic CMS 2010.04.17 (SMExt) Remote Cross-Site Scripting Vulnerability
- [10.06.2011] Pacer Edition CMS 2.1 (l param) Local File Inclusion Vulnerability
- [09.06.2011] Pacer Edition CMS 2.1 Remote XSS POST Injection Vulnerability
- [09.06.2011] Pacer Edition CMS 2.1 (rm) Remote Arbitrary File Deletion Exploit
- [02.06.2011] Ushahidi 2.0.1 (range param) SQL Injection Vulnerability (post-auth)
- [31.05.2011] Kentico CMS <=5.5R2.23 Cross-Site Scripting POST Injection Vulnerability
- [22.05.2011] Tugux CMS 1.2 Multiple Remote Vulnerabilities
- [13.05.2011] DreamBox DM500(+) Arbitrary File Download Vulnerability
- [12.05.2011] Adobe Audition 3.0 (build 7283) Session File Handling Buffer Overflow PoC
- [21.04.2011] Gesytec ElonFmt ActiveX 1.1.14 (ElonFmt.ocx) pid Item Buffer Overflow (SEH)
- [20.04.2011] docuFORM Mercury WebApp 6.16a/5.20 Multiple Cross-Site Scripting Vulnerabilities
- [14.04.2011] Help & Manual Professional Edition 5.5.1 (ijl15.dll) DLL Hijacking Exploit
- [06.04.2011] Anfibia Reactor 2.1.1 (login.do) Remote XSS POST Injection Vulnerability
- [05.04.2011] TutorialMS v1.4 (show) Remote SQL Injection Vulnerability
- [03.04.2011] DoceboLMS 4.0.4 Multiple Stored XSS Vulnerabilities
- [03.04.2011] Antamedia Internet Cafe Software 7.1 Insecure Permissions/DLL Loading
- [25.03.2011] Family Connections CMS 2.3.2 (POST) Stored XSS And XML Injection
- [16.03.2011] Microsoft Source Code Analyzer for SQL Injection 1.3 Improper Permissions
- [16.03.2011] Pointter PHP Content Management System 1.2 Multiple Vulnerabilities
- [11.03.2011] Constructr CMS 3.03 Multiple Remote Vulnerabilities (XSS/SQLi)
- [26.02.2011] eXpert PDF Reader 4.0 NULL Pointer Dereference and Heap Corruption Denial Of Service
- [26.02.2011] Nitro PDF Reader 1.4.0 Remote Heap Memory Corruption / DoS PoC
- [24.02.2011] Elecard MPEG Player 5.7 Local Buffer Overflow PoC (SEH)
- [22.02.2011] WinMerge v2.12.4 Project File Handling Stack Overflow Vulnerability
- [18.02.2011] phpBugTracker 1.0.5 Multiple Reflected XSS Vulnerabilities
- [17.02.2011] GAZie 5.10 (Login parameter) Multiple Remote Vulnerabilities
- [15.02.2011] AutoPlay v1.33 (autoplay.ini) Local Buffer Overflow Exploit (SEH)
- [12.02.2011] MG2 0.5.1 Multiple XSS Vulnerabilities
- [11.02.2011] Pixelpost 1.7.3 Multiple POST Variables SQL Injection Vulnerability
- [11.02.2011] Pixelpost 1.7.3 Multiple Persistent Cross-Site Scripting Vulnerabilities
- [11.02.2011] TaskFreak! v0.6.4 Multiple Cross-Site Scripting Vulnerabilities
- [11.02.2011] Oracle MySQL Eventum 2.3 Remote Script Insertion Vulnerabilities
- [22.01.2011] CultBooking 2.0.4 (lang) Local File Inclusion Vulnerability
- [22.01.2011] CultBooking 2.0.4 (cultbooking.php) Multiple XSS/PD Vulnerabilities
- [10.01.2011] Macro Express Pro 4.2.2.1 MXE File Syntactic Analysis Buffer Overflow PoC

- 2010 -

- [23.12.2010] Embedthis Appweb Web Server 3.2.2-1 (Ejscrip) Remote XSS Vulnerability
- [15.12.2010] MantisBT <=1.2.3 (db\_type) Local File Inclusion Vulnerability
- [15.12.2010] MantisBT <=1.2.3 (db\_type) Cross-Site Scripting & Path Disclosure Vulnerability
- [06.12.2010] MODx Revolution CMS 2.0.4-pl2 Remote XSS POST Injection Vulnerability
- [20.11.2010] Native Instruments Service Center 2.2.5 Local Privilege Escalation Vulnerability
- [20.11.2010] Native Instruments Massive 1.1.4 KSD File Handling Use-After-Free Vulnerability
- [20.11.2010] Native Instruments Kontakt 4 Player NKI File Syntactic Analysis Buffer Overflow PoC

- [20.11.2010] Native Instruments Reaktor 5 Player v5.5.1 Heap Memory Corruption Vulnerability
- [20.11.2010] Native Instruments Traktor Pro 1.2.6 Stack-based Buffer Overflow Vulnerability
- [20.11.2010] Native Instruments Kontakt 4 Player v4.1.3 Insecure Library Loading Vulnerability
- [20.11.2010] Native Instruments Service Center 2.2.5 Insecure Library Loading Vulnerability
- [20.11.2010] Native Instruments Reaktor 5 Player v5.5.1 Insecure Library Loading Vulnerability
- [20.11.2010] Native Instruments Guitar Rig 4 Player v4.1.1 Insecure Library Loading Vulnerability
- [08.11.2010] Nevercenter Silo 2.1.1 Insecure Library Loading Vulnerability
- [22.10.2010] Altova DatabaseSpy 2011 Project File Handling Buffer Overflow Vulnerability
- [15.10.2010] eXV? Content Management System 2.10 Remote XSS Vulnerability
- [14.10.2010] Exponent CMS v0.97 Multiple Vulnerabilities
- [06.10.2010] TomatoCart 1.0.1 (json.php) Remote Cross-Site Scripting Vulnerability
- [01.10.2010] Zen Cart v1.3.9f (typefilter) Local File Inclusion Vulnerability
- [01.10.2010] Zen Cart v1.3.9f Multiple Remote Vulnerabilities
- [21.09.2010] Softek Barcode Reader Toolkit ActiveX 7.1.4.14 (SoftekATL.dll) Buffer Overflow PoC
- [17.09.2010] Netautor Professional 5.5.0 (goback) XSS Vulnerability
- [08.09.2010] Textpattern 4.2.0 (txplib\_db) Null Termination Cross-Site Scripting Vulnerability
- [06.09.2010] MySource Matrix 3.28.3 (height) Remote Reflected XSS Vulnerability
- [01.09.2010] LEADTOOLS ActiveX Common Dialogs 16.5 Multiple Remote Vulnerabilities
- [28.08.2010] LEADTOOLS ActiveX Raster Twain v16.5 (Ltoctwainu.dll) Remote Buffer Overflow PoC
- [26.08.2010] Microsoft Visio 2010 v14.0.4514.1004 (dwmapi.dll) DLL Hijacking Exploit
- [26.08.2010] Nullsoft Winamp 5.581 (wnaspi32.dll) DLL Hijacking Exploit
- [26.08.2010] Microsoft Office PowerPoint 2007 v12.0.4518 (pp4x322.dll) DLL Hijacking Exploit
- [26.08.2010] Media Player Classic 6.4.9.1 DLL Hijacking Exploit
- [26.08.2010] Google Earth v5.1.3535.3218 (quserex.dll) DLL Hijacking Exploit
- [26.08.2010] Corel PHOTO-PAINT X3 v13.0.0.576 (crlrib.dll) DLL Hijacking Exploit
- [26.08.2010] CorelDRAW X3 v13.0.0.576 (crlrib.dll) DLL Hijacking Exploit
- [26.08.2010] Adobe ExtendedScript Toolkit CS5 v3.5.0.52 (dwmapi.dll) DLL Hijacking Exploit
- [26.08.2010] Adobe Extension Manager CS5 v5.0.298 (dwmapi.dll) DLL Hijacking Exploit
- [26.08.2010] Adobe Device Central CS5 v3.0.1.0 (dwmapi.dll) DLL Hijacking Exploit
- [14.08.2010] Sports Accelerator Suite v2.0 (news\_id) Remote SQL Injection Vulnerability
- [13.08.2010] SmartCode ServerX VNC Server ActiveX 1.1.5.0 (scvncsrvx.dll) DoS Exploit
- [04.08.2010] Team Johnlong RaidenTunes 2.1.1 Remote Cross-Site Scripting Vulnerability
- [12.07.2010] Corel Presentations X5 15.0.0.357 (shw) Remote Buffer Preoccupation PoC
- [12.07.2010] Corel WordPerfect Office X5 15.0.0.357 (wpd) Remote Buffer Preoccupation PoC
- [02.07.2010] Xplico 0.5.7 (add.ctp) Remote XSS Vulnerability
- [29.06.2010] Adobe Reader 9.3.2 (CoolType.dll) Remote Memory Corruption / DoS Vulnerability
- [19.06.2010] UK One Media CMS (id) Error Based SQL Injection Vulnerability
- [04.06.2010] Adobe InDesign CS3 INDD File Handling Buffer Overflow Vulnerability
- [26.05.2010] Adobe Photoshop CS4 Extended 11.0 ABR File Handling Remote Buffer Overflow PoC
- [26.05.2010] Adobe Photoshop CS4 Extended 11.0 GRD File Handling Remote Buffer Overflow PoC
- [26.05.2010] Adobe Photoshop CS4 Extended 11.0 ASL File Handling Remote Buffer Overflow PoC
- [11.05.2010] Adobe Shockwave Player 11.5.6.606 (DIR) Multiple Memory Vulnerabilities
- [22.04.2010] EDraw Flowchart ActiveX Control 2.3 (EDImage.ocx) Remote DoS Exploit (IE)
- [22.04.2010] EDraw Flowchart ActiveX Control 2.3 (.edd parsing) Remote Buffer Overflow PoC
- [19.04.2010] AVTECH Software (AVC781Viewer.dll) ActiveX Multiple Remote Vulnerabilities
- [11.04.2010] Aladdin eToken PKI Client v4.5 Virtual File Handling Unspecified Memory Corruption PoC
- [05.03.2010] BS.Player v2.51 build 1022 (Media Library) Remote Buffer Overflow Vulnerability
- [05.03.2010] VLC media player 1.0.5 Goldeneye (bookmarks) Remote Buffer Overflow PoC
- [04.03.2010] J. River Media Jukebox 12 MP3 File Handling Remote Heap Overflow PoC
- [03.03.2010] Deimos Kasa <= 2.58 (table) Local Integer Overflow Vulnerability
- [27.02.2010] ExtCalendar 2.0 Beta 2 (upgrade.php) Remote XSS Vulnerability
- [22.02.2010] Nero Burning ROM 9 (iso compilation) Local Buffer Invasion Proof Of Concept
- [22.02.2010] WampServer 2.0i (index.php) Remote Cross Site Scripting Vulnerability
- [22.02.2010] CableTEL's Triple Play v1.0 (login.php) Remote Login Bypass SQL Injection Vuln

## - 2009 -

- [01.08.2009] Google SketchUp Pro 7.0 (.skp file) Remote Stack Overflow PoC
- [30.07.2009] Epiri Professional Web Browser 3.0 Remote Crash Exploit
- [16.07.2009] Music Tag Editor 1.61 build 212 Remote Buffer Overflow PoC
- [16.07.2009] Zortam MP3 Player 1.50 (m3u) Integer Division by Zero Exploit
- [16.07.2009] Zortam MP3 Media Studio 9.40 Multiple Memory Corruption Vulnerabilities
- [16.07.2009] Zortam ID3 Tag Editor 5.0 Remote Stack Overflow Vulnerability
- [16.07.2009] Audio Editor Pro 2.91 Remote Memory Corruption PoC
- [10.07.2009] eEye Retina WiFi Security Scanner 1.0 (.rws Parsing) Buffer Overflow PoC
- [16.06.2009] Carom3D 5.06 Unicode Buffer Overrun/DoS Vulnerability
- [01.06.2009] Mp3 Tag Assistant Pro 2.92 (tag metadata) Remote Stack Overflow PoC
- [29.05.2009] AIMP 2.51 build 330 (ID3v1/ID3v2 Tag) Remote Stack Buffer Overflow PoC (SEH)
- [08.05.2009] ViPlay3 <= 3.00 (.vpl) Local Stack Overflow PoC
- [06.04.2009] Unsniff Network Analyzer 1.0 (usnf) Local Heap Overflow PoC
- [01.04.2009] QtWeb Internet Browser 2.0 (build 043) Remote Denial of Service Exploit (smile)
- [29.03.2009] PowerCHM 5.7 (hhp) Local Buffer Overflow Exploit
- [17.03.2009] Talkative IRC 0.4.4.16 Remote Stack Overflow Exploit (SEH)
- [12.03.2009] JdKChat v1.5 Remote Integer Overflow PoC
- [20.02.2009] Got All Media 7.0.0.3 (t00t) Remote Denial of Service Exploit
- [04.02.2009] BlazeVideo HDTV Player <= 3.5 PLF Playlist File Remote Buffer Overflow Exploit
- [30.01.2009] Amaya Web Editor 11 Remote SEH Overwrite Exploit
- [26.01.2009] WFTPD Pro Server 3.30.0.1 (pre auth) Multiple Remote Denial of Service Vulnerabilities
- [22.01.2009] FTPShell Server 4.3 (licence key) Remote Buffer Overflow PoC

## - 2008 -

- [24.11.2008] Nero ShowTime 5.0.15.0 m3u Playlist File Remote Buffer Overflow PoC
- [24.10.2008] KVirc 3.4.0 Virgo Remote Format String Exploit PoC
- [14.10.2008] Eserv 3.x FTP Server (ABOR) Remote Stack Overflow PoC
- [03.10.2008] VBA32 Personal Antivirus 3.12.8.x (malformed archive) DoS Exploit
- [17.09.2008] Femitter FTP Server 1.03 (RETR) Remote Denial of Service Exploit PoC
- [11.09.2008] Maxthon Browser 2.1.4.443 UNICODE Remote Denial of Service PoC
- [08.09.2008] SeaMonkey 1.1.11 Remote Denial of Service Exploit PoC
- [06.09.2008] Flock Social Web Browser 1.2.5 (loop) Remote Denial of Service Exploit

- [04.09.2008] [Google Chrome Browser 0.2.149.27 Denial of Service Exploit](#)
- [18.08.2008] [Linux/x86 setuid\(0\) . setgid\(0\) . aslr\\_off 79 Bytes Shellcode](#)
- [18.08.2008] [VUPlayer 2.49 M3U Playlist File Remote Buffer Overflow Exploit](#)
- [10.08.2008] [BlazeDVD 5.0 PLF Playlist File Remote Buffer Overflow Exploit](#)
- [02.07.2008] [CyberLink PowerDVD <= 8.0 Crafted PLS/M3U Playlist File BoF Vulnerability](#)

## • Rete mirabilia

u\_u

## • We Suggest

u\_u

## • Profiles

