

Public Vulnerabilities Discovered Using Dranzer

[Symantec AppStream LaunchObj ActiveX control vulnerable to arbitrary code download and execution](#)

[RealNetworks GameHouse dldisplay ActiveX control stack buffer overflows](#)

[SonicWall NetExtender NELaunchCtrl ActiveX control stack buffer overflow](#)

[Adobe Form Designer and Advanced Form Client ActiveX controls contain multiple buffer overflows](#)

[Novell iPrint Client ActiveX control stack buffer overflows](#)

[SAP AG SAPgui MDrmSap ActiveX control code execution vulnerability](#)

[eBay Enhanced Picture Services ActiveX control buffer overflow](#)

[Macrovision FLEXnet Connect / InstallShield Update Service Agent ActiveX buffer overflows](#)

[SupportSoft ActiveX controls contain multiple buffer overflows](#)

[Macrovision FLEXnet Connect Software Manager DWUpdateService ActiveX control contains dangerous methods](#)

[Microsoft Speech API ActiveX controls contain buffer overflows](#)

[Intuit QuickBooks Online Edition ActiveX control stack buffer overflows](#)

[Gateway CWebLaunchCtl ActiveX control buffer overflow](#)

[IBM Lotus Domino Web Access ActiveX control stack buffer overflows](#)

[Oracle JInitiator ActiveX control stack buffer overflows](#)

[PhotoStockPlus Uploader Tool ActiveX stack buffer overflows](#)

[iseemedia / Roxio / MGI Software LPViewer ActiveX control stack buffer overflows](#)

[Microsoft DXImageTransform Light filter fails to validate input](#)

[SAP AG SAPgui EAI WebViewer3D ActiveX control stack buffer overflow](#)

[Particle Software IntraLaunch Application Launcher ActiveX control fails to restrict access to dangerous methods](#)

[Microsoft Whale Intelligent Application Gateway Whale Client Components ActiveX control stack buffer overflows](#)

[HP Virtual Rooms ActiveX control fails to restrict access to dangerous methods](#)

[ICONICS Dialog Wrapper Module ActiveX control vulnerable to buffer overflow](#)

[Panda Security ActiveScan fails to properly validate downloaded software](#)

[Oracle Siebel Option Pack for IE ActiveX control memory initialization vulnerability](#)

[MarkAny ContentSAFER MASetupCaller ActiveX control arbitrary download and execution](#)

[Cisco AnyConnect Clientless SSL VPN Portforwarder ActiveX control buffer overflow](#)

[AVG Safeguard and Secure Search ActiveX controls provides insecure methods](#)