Dranzer

Dranzer is a tool that enables users to examine effective techniques for fuzz testing ActiveX controls.

Attackers frequently take advantage of vulnerabilities in ActiveX controls to compromise systems using Microsoft Internet Explorer. A programming or design flaw in an ActiveX control can allow an attacker to execute arbitrary code by convincing a user to view a specially crafted web page. Since 2000, we have seen a significant increase in vulnerabilities in ActiveX controls.

We have developed Dranzer, a tool that enables users to examine effective techniques for fuzz testing ActiveX controls. By testing a large number of ActiveX controls, we can provide some insight into the current state of ActiveX security. When we discover new vulnerabilities, we practice coordinated disclosure principles and perform the necessary coordination steps.

We have released Dranzer as an open source project on SourceForge to help developers of ActiveX test their controls in their development processes and to invite community participation in making Dranzer a more effective tool. Users must agree to the terms of a license before installing the tool.

More information about the history, motivations, and rationale for Dranzer is available in the white paper titled Vulnerability Detection in ActiveX Controls through Automated Fuzz Testing.

More information about Dranzer

- Dranzer Blog Posts
- Dranzer Release Notes
- Public Vulnerabilities Discovered Using Dranzer

Download Dranzer

Other Links

- CERTCC/dranzer - GitHub
- Dranzer helps test code for ActiveX vulnerabilities | InfoWorld
- CERT releases Dranzer, a new tool to reduce ActiveX vulnerabilities