Firefox installer DLL hijacking

Archived: 2026-11-20 02:14:27 UTC

Mozilla Foundation Security Advisory 2012-98

Announced
: November 20, 2012

Reporter
: Robert Kugler

Impact
: High

Products
: Firefox, Firefox ESR

Fixed in
: - Firefox 17
- Firefox 18
- Firefox ESR 10.0.11
- Firefox ESR 10.0.12
- Firefox ESR 17.0.1

Description

Security researcher **Robert Kugler** reported that when a specifically named DLL file on a Windows computer is placed in the default downloads directory with the Firefox installer, the Firefox installer will load this DLL when it is launched. In circumstances where the installer is run by an administrator privileged account, this allows for the downloaded DLL file to be run with administrator privileges. This can lead to arbitrary code execution from a privileged account.

Additional vulnerable DLL file names were found and fixed in Firefox 18.0, Firefox ESR 17.0.1, and Firefox ESR 10.0.12 releases.

References

- DLL Hijacking - Firefox installer
- CVE-2012-4206

Source: https://www.mozilla.org/en-US/security/advisories/mfsa2012-98/