GostCrypt Security Bulletin

GST16-1

Security Updates for

DLL Hijacking on GostCrypt, GostCrypt Format and GostCrypt Setup

Published : January 11, 2015
Vulnerabilty identifier : GST16-1
Version : 1.0

Executive Summary

This security update resolves know vulnerabilities in the GostCrypt, GostCrypt Format and GostCrypt Setup binaries for Windows. The vulnerabilities could allow the injection of the following DLL during runtime, involving execution of arbitrary code :

- fmifs.dll
- NetAPI32.dll
- Riched20.dll
- SrClient.dll

Affected software, rate and revisions

The security update is rated important.
Following software are vulnerable :

- GostCrypt 1.0 for Windows
- GostCrypt Format 1.0 for Windows
- GostCrypt Setup 1.0 for Windows

Macintosh and Linux versions are not vulnerable.
New release GostCrypt 1.3 for Windows is patched and not vulnerable.

Vulnerability Details

Vulnerable software is using function *LoadLibrary* to load the different dynamic libraries needed by GostCrypt. This function tries to locate the required library by searching through known directories tree, beginning with the directory from which the application is loaded. By placing a corrupted DLL on the directory, an attacker can run arbitrary code. Using function *LoadLibraryEx* allows specify the directory on which the DLL needs to be exclusively loaded. As all DLLs of GostCrypt are from *System32* directory, the *LoadLibray* function is replaced with its extension.

Acknowledgments

GostCrypt Team would like to thank Stefan Kanthak for reporting this vulnerability.