RBS-2019-011

Innorix InnoFD6 ActiveX Control
Multiple Methods Handling Stack Buffer Overflows
**Vulnerable Program Details**

Details for tested products and versions:

Vendor: Innorix
Product: InnoFD6 ActiveX Control (InnoFD6.dll)
Version: 6.0.4.5150

NOTE: Other versions than the one listed above are likely affected.

**Credits**

Carsten Eiram, Risk Based Security
Twitter: @RiskBased

**Impact**

The InnoFD6 ActiveX control (InnoFD6.dll) contains multiple stack-based buffer overflows that may allow an attacker to compromise a user’s system.

**Vulnerability Details**

**DownloadAndOpen() Method Stack Buffer Overflow**

The ActiveX control provides the DownloadAndOpen() method, which accepts one mandatory argument and three optional ones as defined below:

```c
[id(0x0000025b), helpstring("¸Þ¼µå DownloadAndOpen")]
void DownloadAndOpen(
    [in] BSTR bstrURL,
    [in, optional, defaultvalue("")] BSTR bstrFilename,
    [in, optional, defaultvalue(0)] int64 nFilesize,
    [in, optional, defaultvalue(-1)] VARIANT_BOOL bOverwrite);
```

When the DownloadAndOpen() method is called, the function responsible for handling it in InnoFD6.dll eventually copies the “bstrURL” argument into a 2086 wide-character stack buffer via a call to lstrncpyW().

```
.text:10031BA6             mov     ebx, [ebp+14D0h+bstrURL]
.text:10031BAC             push    esi
.text:10031BAD             mov     esi, [ebp+14D0h+pThis]
```
As no bounds checks are performed, this may lead to a stack-based buffer overflow.

**SingleDownload() Method Stack Buffer Overflow**

The ActiveX control provides the SingleDownload() method, which accepts one mandatory argument and two optional ones as defined below:

```c
void SingleDownload(
    [in] BSTR bstrURL,
    [in, optional, defaultvalue("") BSTR bstrFilename,
    [in, optional, defaultvalue(0)] int64 nFilesize);
```

When the SingleDownload() method is called, the function responsible for handling it in InnoFD6.dll eventually copies the “bstrURL” argument into a 2086 wide-character stack buffer via a call to lstrcpyW().

As no bounds checks are performed, this may lead to a stack-based buffer overflow.

**AppendFile() Method Stack Buffer Overflow**

The ActiveX control provides the AppendFile() method, which accepts one mandatory argument and two optional ones as defined below:
void AppendFile(
    [in] BSTR bstrURL,
    [in, optional, defaultvalue(""), [in, optional, defaultvalue(0)] int64 varFilesize);

When the AppendFile() method is called, the function responsible for handling it in InnoFD6.dll eventually copies the “bstrURL” argument into a 2086 wide-character stack buffer via a call to lstrcpyW().

As no bounds checks are performed, this may result in a stack-based buffer overflow.

Later in another function the optional “bstrFilename” argument is processed if supplied. Here the filename is copied into a 260 wide-character stack buffer via a call to wcsncpy().
As the supplied size argument to wcsncpy() is the length of the source string, no boundary checks are basically performed. This may result in a stack-based buffer overflow.

**Solution**

The vendor has deprecated the ActiveX control, and KrCERT/CC plans to set the kill-bit.

**References**

RBS: RBS-2019-011

VulnDB: 202035, 202036, 202037, 202038

**Timeline**

- **2019-01-29**: Vulnerabilities discovered.
- **2019-02-01**: Vulnerabilities reported to KrCERT/CC.
- **2019-04-04**: Alerts published to VulnDB customers.
- **2019-05-21**: Publication of this vulnerability report.

---

About Risk Based Security

Risk Based Security offers clients fully integrated security solutions, combining real-time vulnerability and threat data, as well as the analytical resources to understand the implications of the data, resulting in not just security, but the right security.

Company History

Risk Based Security, Inc. (RBS) was established to support organizations with the technology to turn security data into actionable information and a competitive advantage. We do so by enhancing the research available and providing a first of its kind risk identification and evidence-based security management service.

As a data driven and vendor neutral organization, RBS is able to deliver focused security solutions that are timely, cost effective, and built to address the specific threats and vulnerabilities most relevant to the organizations we serve. We not only maintain vulnerability and data breach databases, we also use this information to inform our entire practice.

Solutions

VulnDB - Vulnerability intelligence, alerting, and third party library tracking based on the largest and most comprehensive vulnerability database in the world. Available as feature-rich SaaS portal or powerful API. Vendor evaluations including our Vulnerability Timeline and Exposure Metrics (VTEM), Cost of Ownership ratings, Code Maturity, and Social Risk Scores.

Cyber Risk Analytics - Extensive data breach database including interactive dashboards and breach analytics. Clients are able to gather and analyze security threat and data breach information on businesses, industries, geographies, and causes of loss. It also allows monitoring of domains for data breaches and leaked credentials as well as implementing a continuous vendor management program with our PreBreach data.

YourCISO - Revolutionary service that provides organizations an affordable security solution including policies, vulnerability scans, awareness material, incident response, and access to high quality information security resources and consulting services.

Vulnerability Assessments (VA) and Pentesting - Regularly scheduled VAs and pentests help an organization identify weaknesses before the bad guys do. Managing the most comprehensive VDB puts us in a unique position to offer comprehensive assessments, combining the latest in scanning technology and our own data. Detailed and actionable reports are provided in a clear and easy to understand language.

Security Development Lifecycle (SDL) - Consulting, auditing, and verification specialized in breaking code, which in turn greatly increases the security of products.