RBS-2019-007

FnProWeb ActiveX Control Insecure SetUrlDownLoadStart() Method Arbitrary Code Execution

Vulnerable Program Details

Details for tested products and versions:

Vendor:	Samsung Securities
Product:	FnProWeb ActiveX Control (FnProWeb.ocx)
Version:	1.0.0.5

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

Credits

Carsten Eiram, Risk Based Security
Twitter: @RiskBased

Impact

The FnProWeb ActiveX Control (FnProWeb.ocx) contains an unsafe method as well as a stack-based buffer overflow that may allow an attacker to compromise a user's system.

Vulnerability Details

The FnProWeb ActiveX control provides the SetUrlDownLoadStart() method, which accepts three arguments as defined below:

```
[id(0x00000005)]
void SetUrlDownLoadStart(
                BSTR strUrl,
                BSTR strFileName,
                long nType);
```

Insecure File Download And Execution

The first two arguments are the most interesting. The function that handles calls to the method in FnProWeb.ocx basically creates a new thread that downloads a file from the URL specified by the "strUrl" argument, writes it to disk based on the name in the "strFileName" argument, and then executes it. This allows an attacker to trivally download and execute arbitrary code on a user's system.

Filename Handling Stack Buffer Overflow

The function spawned as a new thread to download and write the file crafts the download path by calling sprintf(). The path is written to a 260 byte stack buffer with one of the components being the “strFileName” argument, which was passed to the SetUrlDownLoadStart() method.

```
.text:100029A5                mov     eax, [ebx+1C4h] ; strFilename
.text:100029AB                lea     ecx, [ebp+szPath] ; char[260]
.text:100029B1                push    eax
.text:100029B2                push    ecx
.text:100029B3                lea     edx, [ebp+szDest] ; char[260]
.text:100029B9                push    offset aSS      ; "%s\\%s"
.text:100029BE                push    edx             ; Dest
.text:100029BF                call    ds:sprintf      ; b0f!
```

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

Solution

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

References

RBS:	RBS-2019-007[1]
VulnDB:	202039, 202040

Timeline

2019-01-28	Vulnerability discovered.
2019-02-01	Vulnerability reported to KrCERT/CC.
2019-04-04	Alerts published to VulnDB customers.
2019-05-21	Publication of this vulnerability report.

[1] https://www.riskbasedsecurity.com/research/RBS-2019-007.pdf

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.