RBS-2019-012

iEBSWAX ActiveX Control
Add() Method Argument Handling Heap Buffer Overflows

Vulnerable Program Details

Details for tested products and versions:

Vendor:	Korea Educational Broadcasting Corporation (EBSi)
Product:	iEBSWAX ActiveX Control (iEBSWAX.dll)
Version:	1.0.0.54

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

Credits

Carsten Eiram, Risk Based Security
Twitter: @RiskBased

Impact

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

Vulnerability Details

The ActiveX control provides the Add() method, which accepts 10 arguments as defined below:

```
[id(0x00000001), helpstring("method Add")]
void Add(
                BSTR Key,
                BSTR cID,
                BSTR cName,
                BSTR kID,
                BSTR kName,
                BSTR StartTime,
                short nTimeRange,
                BSTR URL,
                BSTR LocalFileName,
                BSTR cType);
```

When the Add() method is called, the function responsible for handling it in iEBSWAX.dll eventually allocates and zeroes 1291 bytes of heap memory for a structure to hold the supplied arguments.

```
.text:10002889                mov     esi, 50Bh
```

```
.text:1000288E                  push    esi             ; size_t
.text:1000288F                  call    ??2@YAPAXI@Z    ; operator new(uint)
.text:10002894                  push    esi             ; size_t
.text:10002895                  mov     ebx, eax
.text:10002897                  push    0               ; int
.text:10002899                  push    ebx             ; void *
.text:1000289A                  call    _memset
```

A bit later, the argument is converted from a wide-character string.

```
.text:100028BD                  push    [ebp+Key]       ; lpString
.text:100028C0                  call    esi ; lstrlenW
.text:100028C2                  lea     edi, [eax+eax+2]
.text:100028C6                  mov     eax, edi
.text:100028C8                  add     eax, 3
.text:100028CB                  and     eax, 0FFFFFFFCh
.text:100028CE                  call    __alloca_probe
.text:100028D3                  mov     eax, esp
.text:100028D5                  push    [ebp+CodePage]  ; CodePage
.text:100028D8                  push    edi             ; cbMultiByte
.text:100028D9                  push    [ebp+Key]       ; lpWideCharStr
.text:100028DC                  push    eax             ; lpMultiByteStr
.text:100028DD                  call    unknown_libname_115 ; MFC 3.1-14.0 32bit
.text:100028E2                  mov     edi, [ebp+pThis]
.text:100028E5                  mov     [ebp+Key], eax
```

The length of the converted argument is calculated and then copied into the previously allocated heap-based buffer via a call to memcpy().

```
.text:100028E8                  push    [ebp+Key]       ; char *
.text:100028EB                  call    _strlen
.text:100028F0                  push    eax             ; size_t
.text:100028F1                  push    [ebp+Key]       ; void *
.text:100028F4                  push    ebx             ; void *
.text:100028F5                  call    _memcpy
```

As the length of the source string is used as the size argument, no proper bounds checks are performed. This may lead to a heap-based buffer overflow.

NOTE: Similar vulnerabilities exist when processing any of the other BSTR type arguments.

Solution

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

References

RBS:	RBS-2019-012[1]
VulnDB:	202047, 202048, 202049, 202050, 202051, 202052, 202053, 202054, 202055

Timeline

2019-01-18	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.

[1] https://www.riskbasedsecurity.com/research/RBS-2019-012.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.