RBS-2019-003

D2RCG QRCodeX2 ActiveX Control Make() Method Stack Buffer Overflow

Vulnerable Program Details

Details for tested products and versions:

Vendor:	D2RCG
Product:	QRCodeX2 ActiveX Control (QRCodeX2.ocx)
Version:	1.0.0.1

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

Credits

Carsten Eiram, Risk Based Security
Twitter: @RiskBased

Impact

The QRCodeX2 ActiveX control (QRCodeX2.ocx) contains a stack-based buffer overflow that may allow an attacker to compromise a user's system.

Vulnerability Details

One of the methods provided by the QRCodeX2 ActiveX control is Make(), which accepts a single argument as defined below:

```
[id(0x0000000d)]
VARIANT_BOOL Make(BSTR BarcodeFile);
```

When the method is called, control is transferred to a function in QRCodeX2.ocx that first creates a CString object containing the supplied "BarcodeFile" argument.

```
.text:10001B10 ; int __stdcall M_Make(char *pszBarcodeFile)
.text:10001B10 M_Make          proc near               ; DATA XREF: .rdata:100036D0o
.text:10001B10
.text:10001B10 oCString1       = dword ptr -810h
.text:10001B10 szBuf2          = byte ptr -80Ch        ; char[1024]
.text:10001B10 szBuf1          = byte ptr -40Ch        ; char[1024]
.text:10001B10 var_C           = dword ptr -0Ch
.text:10001B10 var_4           = dword ptr -4
.text:10001B10 pszBarcodeFile  = dword ptr  4
.text:10001B10
```

```
.text:10001B10 this = ebx
.text:10001B10                 push    0FFFFFFFFh
.text:10001B12                 push    offset SEH_10001B10
.text:10001B17                 mov     eax, large fs:0
.text:10001B1D                 push    eax
.text:10001B1E                 mov     large fs:0, esp
.text:10001B25                 sub     esp, 804h
.text:10001B2B                 push    this
.text:10001B2C                 push    esi
.text:10001B2D                 push    edi
.text:10001B2E                 mov     edi, [esp+81Ch+pszBarcodeFile]
.text:10001B35                 mov     this, ecx
.text:10001B37                 push    edi             ; char *
.text:10001B38                 lea     ecx, [esp+820h+oCString1] ; this
.text:10001B3C                 call    ??0CString@@QAE@PBD@Z ; CString::CString(char const *)
```

The supplied argument is then copied to a 1024 byte stack buffer using an inlined strcpy() call without performing any boundary checks.

```
.text:10001B41                 or      ecx, 0FFFFFFFFh
.text:10001B44                 xor     eax, eax
.text:10001B46                 repne scasb
.text:10001B48                 not     ecx
.text:10001B4A                 sub     edi, ecx
.text:10001B4C                 lea     edx, [esp+81Ch+szBuf1] ; char[1024]
.text:10001B53                 mov     eax, ecx
.text:10001B55                 mov     esi, edi
.text:10001B57                 mov     edi, edx
.text:10001B59                 mov     edx, [this+1C0h]
.text:10001B5F                 shr     ecx, 2
.text:10001B62                 rep movsd               ; b0f!
.text:10001B64                 mov     ecx, eax
.text:10001B66                 mov     [esp+81Ch+var_4], 0
.text:10001B71                 and     ecx, 3
.text:10001B74                 rep movsb
```

This can lead to a stack-based buffer overflow and arbitrary code execution.

Solution

The vendor has discontinued this product, and KrCERT/CC plans to set the kill-bit.

References

RBS:	RBS-2019-003[1]
VulnDB:	202017

[1] https://www.riskbasedsecurity.com/research/RBS-2019-003.pdf

Timeline

2019-01-07	Vulnerability discovered.
2019-02-01	Vulnerability reported to KrCERT/CC.
2019-04-04	Alert 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.