RBS-2019-008

Looyu DyLooyu ActiveX Control CreateCom() Method Handling Stack Buffer Overflow

Vulnerable Program Details

Details for tested products and versions:

Vendor:	Looyu
Product:	DyLooyu ActiveX Control (dyLooyu.dll)
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 DyLooyu ActiveX control (dyLooyu.dll) 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 DyLooyu ActiveX Control is `CreateCom()`, which accepts two arguments as defined below:

```
[id(0x00000002), helpstring("method CreateCom")]
IDispatch* CreateCom(
                [in] BSTR name,
                [in] BSTR bversion);
```

When the method is called, the function responsible for handling it eventually ends up calling a function to create a path to a file based on the "name" argument. The function first retrieves the path to the system directory...

```
.text:100018AE ; int __stdcall sub_100018AE(int psz_name, char *psz_bversion, char *pszDest)
.text:100018AE sub_100018AE    proc near               ; CODE XREF: sub_10001951+19p
.text:100018AE
.text:100018AE szPath          = byte ptr -300h        ; char[256]
.text:100018AE szSysDir        = byte ptr -200h        ; char[256]
.text:100018AE tstrFilename    = byte ptr -100h        ; char[256]
.text:100018AE psz_name        = dword ptr  8
```

```
.text:100018AE psz_bversion    = dword ptr  0Ch
.text:100018AE pszDest         = dword ptr  10h
.text:100018AE
.text:100018AE                 push    ebp
.text:100018AF                 mov     ebp, esp
.text:100018B1                 sub     esp, 300h
.text:100018B7                 push    esi
.text:100018B8                 lea     eax, [ebp+szSysDir] ; char[256]
.text:100018BE                 push    0FFh            ; uSize
.text:100018C3                 mov     esi, ecx
.text:100018C5                 push    eax             ; lpBuffer
.text:100018C6                 call    ds:GetSystemDirectoryA
.text:100018CC                 test    eax, eax
.text:100018CE                 jle     short loc_10001949
```

… before it then constructs a path using calls to `sprintf()` without performing any boundary checks.

```
.text:100018D0                 push    [ebp+psz_name]
.text:100018D3                 lea     eax, [ebp+szSysDir] ; char[256]
.text:100018D9                 push    eax
.text:100018DA                 lea     eax, [ebp+szPath] ; char[256]
.text:100018E0                 push    offset aSLdyS   ; "%s\\ldy\\%s"
.text:100018E5                 push    eax             ; char *
.text:100018E6                 call    _sprintf        ; b0f!
.text:100018EB                 add     esp, 10h
.text:100018EE                 lea     eax, [ebp+szPath] ; char[256]
.text:100018F4                 push    [ebp+psz_name]
.text:100018F7                 push    eax
.text:100018F8                 lea     eax, [ebp+tstrFilename] ; char[256]
.text:100018FE                 push    offset aSS      ; "%s\\%s"
.text:10001903                 push    eax             ; char *
.text:10001904                 call    _sprintf        ; b0f!
```

This may allow an attacker to cause a stack-based buffer overflow and gain control of the execution flow by overwriting the return address.

Solution

We are not currently aware of an updated version, and the vulnerable ActiveX control is still available for download. Users are encouraged to delete it from their systems.

References

RBS: RBS-2019-008[1]
VulnDB: 202057

[1] https://www.riskbasedsecurity.com/research/RBS-2019-008.pdf

Timeline

2019-01-31	Vulnerability discovered.
2019-02-01	Vulnerability reported to KrCERT/CC, who sent it to CNCERT.
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.