RBS-2015-005

DBI Technologies Studio Controls for COM ctExplorer ActiveX Control trLoadDirectory() Method Stack Buffer Overflow

Vendor / Product Information

DBI Technologies Inc. is a software development company that offers various products and components to ease application design. One of these products is Studio Controls for COM, which bundles various safe-for-scripting ActiveX controls including ctExplorer.ocx.

Vulnerable Program Details

Details for tested products and versions:

Vendor:	DBI Technologies
Product:	Studio Controls for COM
Version:	1.3.0.1, 1.4.0.0, and 1.7.0.2
Component:	ctExplorer ActiveX Control (ctExplorer.ocx)
Component Version:	4.2.0.0

NOTE: Other versions than the one listed above are likely vulnerable. Furthermore, any 3rd party products designed using the solution and bundling the component may be similarly affected.

Credits

Carsten Eiram, Risk Based Security
Twitter: @RiskBased

Vulnerability Details

DBI Technologies Studio Controls for COM bundles the ctExplorer ActiveX control, which provides the `trLoadDirectory()` method defined as:

```
[id(0x000001a5)]
void trLoadDirectory(
                BSTR strDirectory,
                VARIANT_BOOL bSubDir);
```

The ActiveX control does not perform proper bounds checks when processing an overly long '`strDirectory`' argument passed to the `trLoadDirectory()` method.

```
.text:094BE3C0 ; int __thiscall sub_94BE3C0(COleControl *this, int pszDirectory, int, int)
.text:094BE3C0 sub_94BE3C0     proc near               ; CODE XREF: sub_94BE3C0+1BCp
.text:094BE3C0                                         ; sub_94BE3C0+30Dp ...
.text:094BE3C0
.text:094BE3C0 var_624         = dword ptr -624h
.text:094BE3C0 var_620         = dword ptr -620h
.text:094BE3C0 var_61C         = dword ptr -61Ch
.text:094BE3C0 var_618         = _finddata_t ptr -618h
.text:094BE3C0 szBuf2          = byte ptr -500h        ; char[256]
.text:094BE3C0 szBuf1          = byte ptr -400h        ; char[1024]
.text:094BE3C0 pszDirectory    = dword ptr  4
.text:094BE3C0 arg_4           = dword ptr  8
.text:094BE3C0 arg_8           = dword ptr  0Ch
.text:094BE3C0
.text:094BE3C0                 sub     esp, 624h
.text:094BE3C6                 push    ebx
.text:094BE3C7                 push    ebp
.text:094BE3C8                 push    esi
.text:094BE3C9                 mov     ebp, ecx
.text:094BE3CB                 push    edi
.text:094BE3CC                 mov     edi, [esp+634h+pszDirectory]
.text:094BE3D3                 or      ecx, 0FFFFFFFFh
.text:094BE3D6                 xor     eax, eax
.text:094BE3D8                 repne scasb
.text:094BE3DA                 not     ecx
.text:094BE3DC                 sub     edi, ecx
.text:094BE3DE                 lea     edx, [esp+634h+szBuf2] ; char[256]
.text:094BE3E5                 mov     eax, ecx
.text:094BE3E7                 mov     esi, edi
.text:094BE3E9                 mov     edi, edx
.text:094BE3EB                 lea     edx, [esp+634h+szBuf2] ; char[256]
.text:094BE3F2                 shr     ecx, 2
.text:094BE3F5                 rep movsd               ; b0f!
```

With a specially crafted web page, a context-dependent attacker can cause a stack-based buffer overflow and execute arbitrary code.

Solution

No solution is currently available from the vendor.

References

RBS:	RBS-2015-005[1]
VulnDB:	122325

Timeline

2015-05-06	Vulnerability discovered.
2015-05-07	Vulnerability reported to the vendor.
2015-05-18	2nd attempt at contacting the vendor.
2015-05-20	No response from the vendor. Alert sent to RBS VulnDB clients.
2018-05-23	Publication of this vulnerability report.

[1] https://www.riskbasedsecurity.com/research/RBS-2015-005.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.