RBS-2019-005

GKDirCtrl ActiveX Control Insecure ExecTheViewer() Method Arbitrary Command Execution

Vulnerable Program Details

Details for tested products and versions:

Vendor:	Korean Intellectual Property Office
Product:	GKDirCtrl ActiveX Control (GKDirCtrl.ocx)
Version:	2.0.0.0

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

Credits

Carsten Eiram, Risk Based Security
Twitter: @RiskBased

Impact

The GKDirCtrl ActiveX control (GKDirCtrl.ocx) contains an unsafe method that may allow an attacker to execute arbitrary commands on a user's system.

Vulnerability Details

One of the methods provided by the GKDirCtrl ActiveX control is ExecTheViewer(), which accepts two arguments as defined below:

```
[id(0x00000012)]
short ExecTheViewer(
                BSTR Viewer_Path,
                BSTR Exec_Args);
```

When the method is called, the function responsible for handling it in GKDirCtrl.ocx passes the two arguments via “lpFile” and “lpParameters” to ShellExecuteA() without performing any validation.

```
.text:10002A90 ; int __stdcall M_ExecTheViewer(LPCSTR pszViewer_Path, LPCSTR pszExec_Args)
.text:10002A90 M_ExecTheViewer proc near               ; DATA XREF: .rdata:10005870o
.text:10002A90
.text:10002A90 pszViewer_Path  = dword ptr  4
.text:10002A90 pszExec_Args    = dword ptr  8
.text:10002A90
```

```
.text:10002A90                  mov     eax, [esp+pszExec_Args]
.text:10002A94                  mov     ecx, [esp+pszViewer_Path]
.text:10002A98                  push    5                ; nShowCmd
.text:10002A9A                  push    0                ; lpDirectory
.text:10002A9C                  push    eax              ; lpParameters
.text:10002A9D                  push    ecx              ; lpFile
.text:10002A9E                  push    offset Operation ; "open"
.text:10002AA3                  push    0                ; hwnd
.text:10002AA5                  call    ds:ShellExecuteA
.text:10002AAB                  neg     eax
.text:10002AAD                  sbb     eax, eax
.text:10002AAF                  inc     eax
.text:10002AB0                  retn    8
```

This allows an attacker to execute arbitrary commands with arguments on the system.

Solution

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

References

RBS:	RBS-2019-005[1]
VulnDB:	202034

Timeline

2019-01-31	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.

[1] https://www.riskbasedsecurity.com/research/RBS-2019-005.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.