RBS-2019-004

PS_NTS ActiveX Control ps_ntscrypto.dll
Relative Distinguished Names Handling Buffer Overflows
Vulnerable Program Details

Details for tested products and versions:

Vendor: SG Co Ltd.
Product: PS_NTS ActiveX Control (PS_NTS.dll)
Version: 4.1.1.4
Component: ps_ntscrypto.dll
Component Version: 4.1.1.3

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

Credits

Carsten Eiram, Risk Based Security
Twitter: @RiskBased

Impact

The PS_NTS ActiveX control bundles the ps_ntscrypto.dll library, which contains various buffer overflows that may allow an attacker to compromise a user’s system.

Vulnerability Details

The ps_ntscrypto.dll library bundled with the PS_NTS ActiveX control exports various crypto functionality, where some of the functions of particular interest to these vulnerabilities are e.g. ps_req_auth_string() and ps_get_session_key(). The exported functions can be reached via methods provided by the ActiveX control such as PsWebClientReqAuth() and PsWebGetSKey().

The PsWebClientReqAuth() method for authenticating a client is defined as follows:

```csharp
[id(0x000000e), helpstring("method PsWebClientReqAuth")]
BSTR PsWebClientReqAuth(
    [in] BSTR inCname,
    [in] BSTR inPasswd,
    [in] BSTR inRdname);
```
The PsWebGetSKey() method for getting a session key is defined as follows:

```c
[id(0x00000028), helpstring("method PsWebGetSKey")]
BSTR PsWebGetSKey([in] BSTR RDNAME);
```

In both cases, the argument of interest is ‘inRdname’ or ‘RDNAME’, which is intended to supply a list of relative distinguished names.

When either of these two methods is called, the function in PS_NTS.dll that is responsible for handling the call eventually transfers control to the corresponding exported function in ps_ntscrypto.dll along with the supplied arguments. Both functions end up calling a function to parse the supplied relative distinguished name string. This function allocates a 201 byte buffer on the heap and checks if the supplied string starts with “cn=“.

```asm
; int __cdecl ConstructRDName(char *pszinRdname)
ConstructRDName proc near                   ; CODE XREF: sub_22D1CD0+53p
        sub     esp, 978h
        push    ebx
        push    ebp
        push    esi
        push    edi
        mov     ecx, 19h
        xor     eax, eax
        lea     edi, [esp+988h+pszinRdname]  ; char[2000]
        mov     edx, 0
        mov     eax, [esp+988h+pszinRdname]
        rep stosd
        mov     eax, [esp+988h+pszinRdname]
        rep stosd
        mov     eax, [esp+988h+pszinRdname]
        rep stosd
        mov     eax, [esp+988h+pszinRdname]
        rep stosd
        mov     eax, [esp+988h+pszinRdname]
        rep stosd
        mov     eax, [esp+988h+pszinRdname]
        rep stosd
\textendasm
```

2019-05-21
If so, the string is copied to the previously allocated heap buffer without performing any boundary checks. This may cause a heap-based buffer overflow.

If, however, the string did not start with “cn=”, the function checks if “/C=” can be found anywhere in the supplied string.
If "/C=" cannot be found, the string is copied into the heap buffer without performing any boundary checks. This may also lead to a heap-based buffer overflow.

If the string does contain "/C=", a check is performed to see if another "/" character exists later in the string.

If so, the whole argument passed to "/C=" is copied into a 4 byte stack buffer without performing any boundary checks. This may lead to a stack-based buffer overflow.
If the string does contain a "/" character after "C=", the length of the argument to that parameter is calculated before calling strncpy() to copy the argument into the 4 byte stack buffer. As the length of the source string is used as size argument, a stack-based buffer overflow may also occur here.

Similar flawed copy operations are later performed for "O="; "OU="; and "CN=" when present in the string. These may all result in stack-based buffer overflows.

Solution

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

References

RBS: RBS-2019-004
VulnDB: 202041, 202042, 202043, 202044, 202045, 202046

Timeline

2019-01-29 Vulnerability discovered.
2019-02-01 Vulnerability reported to KrCERT/CC.
2019-04-04 Alerts 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.