tenable

SolarWinds Dameware DoS

High

← View More Research Advisories

Synopsis

When the DWRCS.exe 'Allow only FIPS Mode' setting is enabled, DWRCRSA.dll is loaded to perform ECDH key exchange. During the key exchange, the client signs the ECDH shared secret with an EC private key and sends the server both the signature and the EC public key so that the server can verify the signature. Inside the key exchange message, an unauthenticated, remote attacker can specify a large 'SigPubkeyLen' field (i.e., 0x1fffff) to cause a buffer over-read/over-write condition in DWRCRSA.dll:

```
.text:100026E4      mov     edi, [esp+343Ch+msg.SigPubkeyLen] ; attacker-controlled
.text:100026EB      push    edi    ; size_t
.text:100026EC      lea     eax, [esp+3440h+msg.SigPubkey] ; stack buffer; received msg
.text:100026F3      push    eax    ; void *
.text:100026F4      lea     ecx, [esi+OBJ_205C.SigPubkey] ; heap buffer
.text:100026FA      push    ecx    ; void *
.text:100026FB      call    _memcpy
```

The key exchange msg has the following format:

```
// used for DH/ECDH key exchange
// msg_len: 0x2c2c
// le = little endian
struct msg_000105b9
{
        le32 MsgType;   // must be 0x000105b9
        byte unk[4];
        le32 status;   // 0 - no error
        byte msg[0x1000];       // error msg
        byte SrvPubKey[0x400];
        le32 SrvPubKeyLen;
        le32 CltSharedSecretLen;    // length of client-computed DH/ECDH shared secret
        le32 CltSharedSecretByteSum;// client-computed sum of all bytes in the secret
        byte CltPubKey[0x400];
        le32 CltPubKeyLen;
        le32 SrvSharedSecretLen; // length of server-computed DH/ECDH shared secret
        le32 SrvSharedSecretByteSum;// server-computed sum of all bytes in the secret
        byte Signature[0x800];  // client-generated signature of the shared secret
        le32 SignaturLen;
        byte SigPubkey[0x800];  // public key to verify the signature
        le32 SigPubkeyLen;
        byte unk[0x400];
};
```

If the msg.SigPubkeyLen field is greater than 0x800, it can cause a buffer over-read on the stack buffer msg.SigPubkey and a buffer over-write on the 0x800-byte SigPubkey local buffer located at offset 0x143c of a 0x205c-byte structure on the heap.

The attached PoC can be used to terminate DWRCS.exe:

```
python dameware_dwrcrsa_sigpubkey_bof.py -t  -p 6129
```

Solution

Upgrade to 12.1.1

Proof of Concept

https://github.com/tenable/poc/blob/master/Solarwinds/Dameware/dameware_dwrcrsa_sigpubkey_bof.py

Additional References

https://documentation.solarwinds.com/en/Success_Center/dameware/Content/Release_Notes/Dameware_12-1-1_release_notes.htm

Disclosure Timeline

01/15/2020 - Vulnerability disclosed. 90-day date is April 14, 2020.
01/15/2020 - Received automated response asking to submit via form. Submitted.
01/15/2020 - SolarWinds asks for PoC to be resent. Tenable does so.
01/20/2020 - SolarWinds validates report. Engineers are working on a fix. They will update us as the team makes progress.
01/20/2020 - Tenable acknowledges.
02/11/2020 - Tenable asks for an update.
02/11/2020 - SolarWinds plans to release a fix around end of March / early April.
02/11/2020 - Tenable acknowledges.
03/19/2020 - SolarWinds is still working on it, and plans to fix in the next release.
03/19/2020 - Tenable asks if a more definitive release date has been decided on.
03/19/2020 - SolarWinds is keeping a close eye on it.
04/06/2020 - Tenable asks for an update.
04/06/2020 - SolarWinds says they released a fix on April 2.

tenable

For more details on submitting vulnerability information, please see our Vulnerability Reporting Guidelines page.

If you have questions or corrections about this advisory, please email advisories@tenable.com

Risk Information

CVE ID: CVE-2020-5734
Tenable Advisory ID: TRA-2020-19
CVSSv2 Base / Temporal Score: 7.1 / 5.6
CVSSv2 Vector: (AV:N/AC:M/Au:N/C:N/I:N/A:C)
Affected Products: SolarWinds Dameware 12.1 Hotfix 3
Risk Factor: High

Advisory Timeline

04/06/2020 - Advisory published

FEATURED PRODUCTS

Tenable One Exposure Management Platform

Tenable.cs Cloud Security

Tenable.io Vulnerability Management

Tenable.io Web App Scanning

Tenable.asm External Attack Surface

Tenable.ad Active Directory

Tenable.ot Operational Technology

Tenable.sc Security Center

Tenable Lumin

Nessus

→ View all Products

FEATURED SOLUTIONS

Application Security

Building Management Systems

Cloud Security Posture Management

Compliance

Exposure Management

Finance

Healthcare

IT/OT

Ransomware

State / Local / Education

US Federal

Vulnerability Management

Zero Trust

→ View all Solutions

CUSTOMER RESOURCES

Resource Library

Community & Support

Customer Education

Tenable Research

Documentation

Trust and Assurance

Nessus Resource Center

Cyber Exposure Fundamentals

System Status

CONNECTIONS

Blog