



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

OK

Do not sell or share my personal information

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

Green Dam 3.17 (Windows XP SP2) - 'URL' Remote Buffer Overflow

EDB-ID:

8938

CVE:

EDB Verified: 

Author:

[SEER\[N.N.U\]](#)

Type:

[REMOTE](#)

Exploit:  



Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >



Green Dam remote buffer overflow exploit

"Green Dam" is a software used for monitoring and anti-pornography, popularizing by Chinese government. After July 1st, it will be forced to install on all new Chinese PCs. Now it already has 50 million copies in China. In order to monitor the URL that user is exploring, Green Dam injected the browser process. When Green Dam is trying to handle a long URL, a stack overflow will occur in the browser process. This exploit can be used for exploitation on IE, on those computers installed Green Dam. I used the .net binary to deploy shellcode, for it's more stable than Heap Spray, and able to bypass DEP and ASLR on Vista. The exploit page contains a .net control, so it should be published on IIS.

```
---seer[N.N.U]
```

<https://gitlab.com/exploit-database/exploitdb-bin-splotts/-/raw/main/bin-splotts/8938.zip> (2009-green-dam.zip)



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

