



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

# 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:**  

**Platform:**

[WINDOWS](#)

**Date:**

2009-06-12

**Vulnerable App:** 



 EXPLOIT DATABASE EXPLOITS GHDB PAPERS SHELLCODES SEARCH EDB SEARCHSPOIT MANUAL SUBMISSIONS ONLINE TRAINING

## 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)

```
# milw0rm.com [2009-06-12]
```

Tags:

Advisory/Source: [Link](#)

Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)[PRIVACY](#)[ABOUT US](#)[FAQ](#)[COOKIES](#)

©

[OffSec Services Limited](#) 2026. All rights reserved.