Analysis of the Green Dam Censorware System

Scott Wolchok, Randy Yao, and J. Alex Halderman
Computer Science and Engineering Division
The University of Michigan

Revision 2.41 – June 11, 2009

***Update: Addendum 1 added June 18, 2009**

Summary We have discovered remotely-exploitable vulnerabilities in Green Dam, the censorship software reportedly mandated by the Chinese government. Any web site a Green Dam user visits can take control of the PC.

According to press reports, China will soon require all PCs sold in the country to include Green Dam. This software monitors web sites visited and other activity on the computer and blocks adult content as well as politically sensitive material.

We examined the Green Dam software and found that it contains serious security vulnerabilities due to programming errors. Once Green Dam is installed, any web site the user visits can exploit these problems to take control of the computer. This could allow malicious sites to steal private data, send spam, or enlist the computer in a botnet. In addition, we found vulnerabilities in the way Green Dam processes blacklist updates that could allow the software makers or others to install malicious code during the update process.

We found these problems with less than 12 hours of testing, and we believe they may be only the tip of the iceberg. Green Dam makes frequent use of unsafe and outdated programming practices that likely introduce numerous other vulnerabilities. Correcting these problems will require extensive changes to the software and careful retesting. In the meantime, we recommend that users protect themselves by uninstalling Green Dam immediately.

Introduction

According to recent news reports (NYT, WSJ), the Chinese government has mandated that, beginning July 1, every PC sold in China must include a censorship program called Green Dam. This software is designed to monitor Internet connections and text typed on the computer. It blocks undesirable or politically sensitive content and optionally reports it to authorities. Green Dam was developed by a company called Jin Hui and is available as a free download. We examined version 3.17.

Green Dam displays this message when it detects banned phrases.

How Green Dam Works

The Green Dam software filters content by blocking URLs and website images and by monitoring text in other applications. The filtering blacklists include both political and adult content. Some of the blacklists appear to have been copied from American-made filtering software.

Image filter Green Dam includes computer vision technology used to block online images containing nudity. The image filter reportedly works by flagging images containing large areas of human skin tone, while making an exception for close-ups of faces. We've found that the program contains code libraries and a configuration file from the open-source image recognition software OpenCV.

Text filter Green Dam scans text entry fields in various applications for blocked words, including obscenities and politically sensitive phrases (for example, references to Falun Gong). Blacklisted terms are contained in three files, encrypted with a simple key-less scrambling operation. We decrypted the contents of these files: xwordl.dat, xwordm.dat, and xwordh.dat. We also found what appears to be a word list for a more sophisticated sentence processing algorithm in the unencrypted file FalunWord.lib. When Green Dam detects these words, the offending program is forcibly closed and an error image (shown above) is displayed.

URL filter Green Dam filters website URLs using patterns contained in whitelist and blacklist files (`*fil.dat`, `adwapp.dat`, and `TrustUrl.dat`). These files are encrypted with the same keyless scrambling operation as the blacklists for the text filter. Five of the blacklists correspond to the categories in the content filtering section of Green Dam's options dialog (shown below).

We found evidence that a number of these blacklists have been taken from the American-made filtering program CyberSitter. In particular, we found an encrypted configuration file, wfileu.dat, that references these blacklists with download URLs at CyberSitter's site. We also found a setup file, xstring.s2g, that appears to date these blacklists to 2006. Finally, csnews.dat is an encrypted 2004 news bulletin by CyberSitter. We conjecture that this file was accidentally included because it has the same file extension as the filters.

Security Problems

After only one day of testing the Green Dam software, we found two major security vulnerabilities. The first is an error in the way the software processes web sites it monitors. The second is a bug in the way the software installs blacklist updates. Both allow remote parties to execute arbitrary code and take control of the computer.

Web Filtering Vulnerability

Green Dam intercepts Internet traffic and processes it to see whether visited web sites are blacklisted. In order to perform this monitoring, it injects a library called `SurfGd.dll` into software that uses the socket API. When a user access a web site, this code checks the address against the blacklist and logs the URL.

We discovered programming errors in the code used to process web site requests. The code processes URLs with a fixed-length buffer, and a specially-crafted URL can overrun this buffer and corrupt the execution stack. Any web site the user visits can redirect the browser to a page with a malicious URL and take control of the computer.

We have constructed a demonstration URL that triggers this problem. If you have Green Dam installed, clicking the button on our **demonstration attack page** will cause your browser (or tab) to crash.

This proof-of-concept shows that we are able to control the execution stack. An actual attacker could exploit this to execute malicious code.

Green Dam's design makes this problem exploitable from almost any web browser. At this time, the surest way for users to protect themselves is to uninstall Green Dam.

Blacklist Update Vulnerability

We found a second problem in the way Green Dam reads its filter files. This problem would allow Green Dam's makers, or a third-party impersonating them, to execute arbitrary code and install malicious software on the user's computer after installing a filter update. Users can enable automatic filter updates from the Green Dam configuration program.

Green Dam reads its filter files using unsafe C string libraries. In places, it uses the `fscanf` function to read lines from filter files into a fixed-length buffer on the execution stack. This creates classic buffer-overflow vulnerabilities. For example, if a line in the file `TrustUrl.dat` exceeds a certain fixed length, the buffer will be overrun, corrupting the execution stack and potentially giving the attacker control of the process.

The filter files can be replaced remotely by the software maker if the user has enabled filter updates. The updates could corrupt these vulnerable files to exploit the problems we found. This could allow Green Dam's makers to take control of any computer where the software is installed and automatic filter updates are enabled. Furthermore, updates are delivered via unencrypted HTTP, which could allow a third party to impersonate the update server (for example, by exploiting DNS vulnerabilities) and take control of users' computers using this attack.

Removing Green Dam

Green Dam allows users who know its administrator password to uninstall the software. We tested the uninstaller and found that it appears to effectively remove Green Dam from the computer. However, it fails to remove some log files, so evidence of users' activity remains hidden on the system.

In light of the serious vulnerabilities we outlined above, the surest way for users to protect themselves is to **remove the software immediately** using its uninstall function.

Conclusion

Our brief testing proves that Green Dam contains very serious security vulnerabilities. Unfortunately, these problems seem to reflect systemic flaws in the code. The software makes extensive use of programming techniques that are known to be unsafe, such as deprecated C string processing functions including `sprintf` and `fscanf`. These problems are compounded by the design of the program, which creates a large attack surface: since Green Dam filters and processes all Internet traffic, large parts of its code are exposed to attack.

If Green Dam is deployed in its current form, it will significantly weaken China's computer security. While the flaws we discovered can be quickly patched, correcting all the problems in the Green Dam software will likely require extensive rewriting and thorough testing. This will be difficult to achieve before China's July 1 deadline for deploying Green Dam nationwide.

Additional Screenshot

Users can configure which categories of web sites are blocked by Green Dam.
Additional filters are used to block adult and politically-sensitive terms in text entry fields.

Addendum 1: Green Dam Quietly Patched; Still Vulnerable — June 18, 2009

Following our initial analysis, the makers of Green Dam have released at least one security update and two filter updates. These updates address the original web filtering security vulnerability we described above, disable certain blacklists that were copied from the CyberSitter program, and bring the software into compliance with the OpenCV license.

Unfortunately, we have discovered an additional remotely-exploitable security vulnerability in the patched version. Even with the updated version installed, any web site a user visits can exploit this problem to take control of the computer. We continue to recommend that users protect themselves by uninstalling Green Dam immediately.

While Green Dam's developers have patched the software quickly, the program's continuing vulnerability suggests that its security problems run deep. We fear that the deeper problems cannot be resolved in time for the July 1 deadline for PC makers to distribute Green Dam on all new PCs sold in China.

Green Dam Security Patch

On June 17, we observed that the Green Dam installer had been updated to correct the web filtering vulnerability that we described in our original report. The update appears to have been released at around 12:00 GMT on June 13. We do not know why the update seems to have been deployed silently; the program is still marked as version 3.17, and we have seen no official announcement of the change. The installer we examined previously is 10,355,637 bytes in size and has the SHA-1 hash `4aaa6cec69b4dfd952eda3512a0b45c1f34a0f7c`, and the new installer is 10,200,230 bytes in size and has the SHA-1 hash `ee93d0ead4982b53d489b4766d6f96e7618fcd6e`. Since these changes do not carry an official version number, we will refer to them as version 3.17a. So far, the new version is only available by downloading a fresh copy of the software from the maker's web site. The changes are not currently being distributed through the software's internal update mechanism.

Green Dam 3.17a has been modified to address several security bugs, including the original demonstration attack we described above. Despite

these attempts to make the software secure, we found a new remotely-exploitable vulnerability in the patched program. It took us just over an hour to find this new vulnerability and approximately five hours to develop a demonstration.

New Web Filtering Vulnerability

Green Dam intercepts Internet traffic using a library called `SurfGd.dll`. Even after the security patch, `SurfGd.dll` uses a fixed-length buffer to process web site requests, and malicious web sites can still overrun this buffer to take control of execution. The program now checks the lengths of the URL and the individual HTTP request headers, but the sum of the lengths is erroneously allowed to be greater than the size of the buffer. An attacker can compromise the new version by using both a very long URL and a very long "Host" HTTP header. The pre-update version 3.17, which we examined in our original report, is also susceptible to this attack.

We have implemented a **second demonstration attack** for this new vulnerability. The page includes a Flash applet that sends a malformed HTTP request to our server. Your browser or tab should crash immediately upon loading the demonstration page if you are running Green Dam 3.17 or 3.17a and have Flash installed. While our demonstration only causes a crash, a real malicious web site could exploit this vulnerability to take control of the computer. We continue to recommend that users uninstall Green Dam immediately to protect themselves.

While our demonstration page uses Flash, this vulnerability is not limited to computers with Flash installed. Attacks are also possible using other browser plugins such as SilverLight or Java. Worse, because Green Dam monitors *every* program that uses the socket API, it will attempt to filter any outgoing message that is structured like an HTTP request, whether or not it actually came from a web browser. Therefore, any program that can be made to send attacker-controlled data over TCP is exposed to both of the web filtering vulnerabilities. We anticipate possible exploits in a variety of networked programs.

We are encouraged that Green Dam's developers have updated the program so quickly. This shows that they take security seriously. Yet even after the recent fix, it is still possible for any web site a Green Dam user visits to exploit other security problems to take control of the computer. As we stated in our original report, the program makes use of insecure programming practices, and there are likely to be more undiscovered problems. Consequently, making Green Dam safe will require substantial changes and careful retesting. It is unlikely that the required changes can be completed in the 12 days remaining before China's July 1 deadline for mandatory distribution of Green Dam with new PCs.

Updates to Blacklists, Whitelists, and Documentation

Green Dam's makers have released two filter updates through the software's internal update mechanism. These updates are not installed automatically by default, but users can apply them by clicking a button in Green Dam's configuration program or enabling automatic updates within the program. Update 3.173 was released on or around June 12, and 3.174 was released on or around June 17.

Changes in 3.173

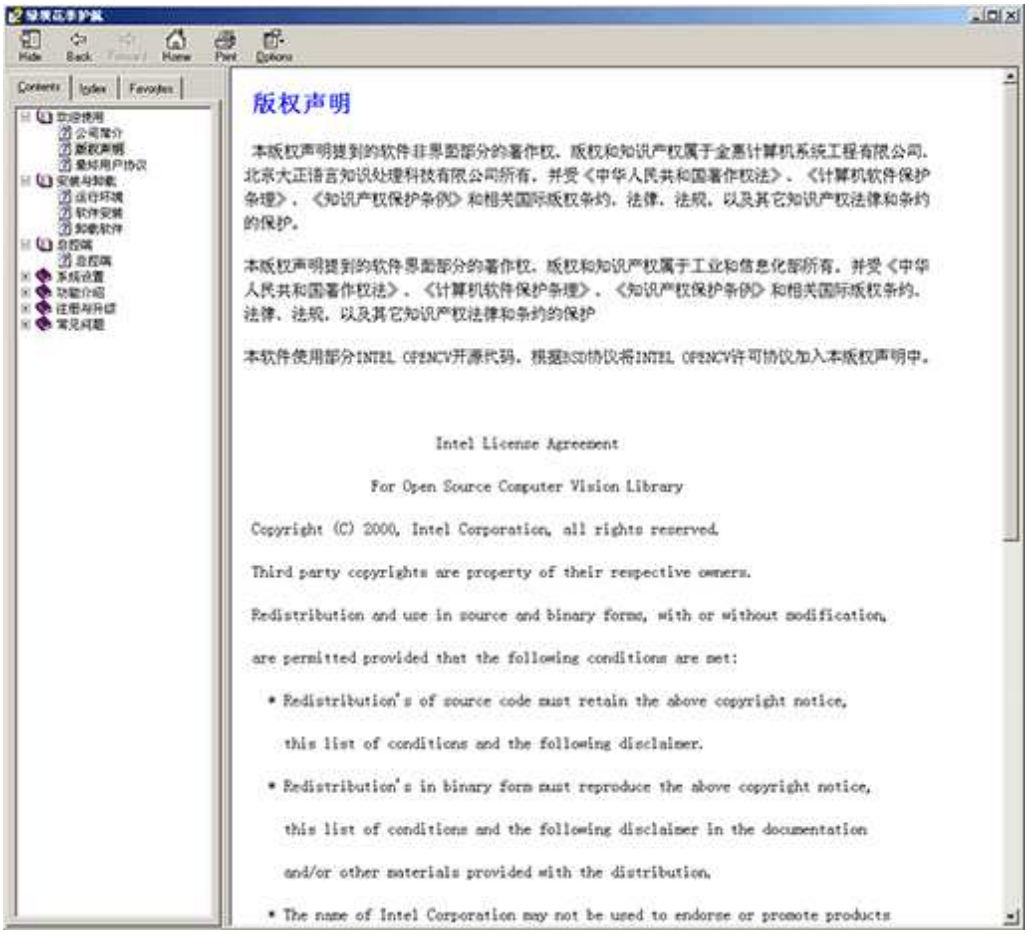
With the 3.173 update installed, Green Dam no longer appears to employ the blacklist files derived from CyberSitter. Instead, it uses an updated version of the `adwapp.dat` blacklist. This list does not seem to be based on CyberSitter: it is over 6000 lines long and contains only five lines in common with any of the CyberSitter blacklists.

By examination of the update file (`kwupdate.dat`), we have established that version 3.173 moved the blacklist files `auctfil.dat`, `bsnlist.dat`, and `gblfil.dat` from `C:\Windows\system32` to `C:\Windows`, and it updated `wfile.dat`, `TrustUrl.dat`, and `adwapp.dat`. The developers added three new entries to `adwapp.dat`: two pornographic sites and the site cmd5.com, which is currently hosting directions on how to change the Green Dam password back to the default. The updates to `wfile.dat` disable the CyberSitter blacklists, leaving only the `adwapp.dat` blacklist active. However, the blacklists copied from CyberSitter continue to be present on the computer following the update, and several of the CyberSitter blacklists are still used in the 3.17a version of Green Dam now being distributed on the maker's web site.

The update also removed 603 entries from `TrustUrl.dat`, a whitelist of sites that are not subject to filtering. Notable entries on the whitelist include aol.com, ibm.com, download.com, abcnews.com, symantec.com, dell.com, china.com, zdnet.com, *.gov.cn, apple.com, filterdam.com, lssw365.*, doubleclick.net, time.com, nokia.com.cn, amazon.com, ebay.com.cn, icq.com, and tucows.com. Curiously, “lssw365” is whitelisted for all top level domains, exempting them from filtering. This includes the site lssw365.org, a Chinese site dedicated to opposing Green Dam.

Changes in 3.174

The 3.174 update changed the program's help file, `kw.chm`, and moved that file from `C:\Windows` to `C:\Windows\Help`. The update added the license text required for the OpenCV open-source project to Green Dam's help, as shown in the screenshot below:



Update 3.174 added the OpenCV license agreement to Green Dam's help file (click to enlarge).

OpenCV is an open-source computer vision package developed by Intel. Green Dam uses it to try to recognize online images that contain nudity. OpenCV is distributed under a license that allows free commercial and educational use, but requires that programs using it include a copy of the license text. We examined Green Dam and found that it contains code libraries and a configuration file derived from version 1.0rc1 of OpenCV, confirming earlier reports on SourceForge. In particular, we found striking similarities between `xcore.dll`, `Xcv.dll`, and `Xtool.dll` from Green Dam and `cxcore099.dll`, `cv099.dll`, `highgui099.dll` from OpenCV 1.0rc1, respectively. Furthermore, Green Dam's `XFimage.xml` is identical to `haarcascade_frontalface_alt2.xml`, except that the license at the top of `haarcascade_frontalface_alt2.xml` (lines 2-44) is not present in `XFimage.xml`.

While the 3.174 filter update added the required license, Green Dam's use of OpenCV prior to version 3.174 may be in violation of OpenCV's license. The license still does not appear in the 3.17a version of Green Dam now being distributed on the maker's web site.

Acknowledgments

We wish to thank our colleagues at the University of Michigan who alerted us to Green Dam and assisted with translation.

Contacting the Authors

Please send questions or comments to Professor J. Alex Halderman.