Das Problem mit den Pipes

Ursprünglich veröffentlicht in Amiga Magazin 02/2002

Großalarm?

Anfang November wurde in einigen Web-Foren und auf verschiedenen News-Seiten im Internet auf eine schwerwiegende Sicherheitslücke in Amiga Internet Programmen aufmerksam gemacht. Dabei wurde mit teilweise recht reißerischen Schlagzeilen nicht gegeizt.

Eine erste Bestandsaufnahme ergibt tatsächlich ein erschreckendes Bild: Unter gewissen Umständen wäre es einem potentiellen Angreifer möglich, auf einem Amiga Programme zu starten - und zwar ohne jegliches Zutun des Besitzers. Dabei stünden ihm sogar etliche verschiedene Möglichkeiten offen, um das gewünschte Ziel zu erreichen. Welche unangenehmen Folgen das haben könnte, wird sehr schnell klar, wenn man an Shell-Befehle wie `DELETE` denkt: Die Befehlsfolge

```
delete SYS:#? ALL FORCE QUIET
```

würde beispielsweise praktisch den gesamten Inhalt Ihrer Bootpartition löschen.

Es gibt jedoch keinen Grund, in Panik zu verfallen: Mit dem entsprechenden Wissen ist es relativ einfach, alle Lücken zu schließen - und viele von Ihnen sind von dem Problem wahrscheinlich gar nicht direkt betroffen.

Beachtlich ist bei der ganzen Thematik viel eher die Tatsache, dass die im Folgenden erläuterten Sicherheitslücken bereits seit mehreren Jahren bekannt sind. Zumindest gibt Vaporware (Voyager, AmIRC, mFTP…) an, dass ihre Programme bereits seit längerem gegen die hier beschriebenen Angriffe immun sind.

Wann ist ein Amiga angreifbar ?

Zunächst einmal gilt: Angreifbar sind nur Rechner, auf denen neben dem Standard „Pipe“-Gerät zusätzlich in der Funktionalität erweiterte Clones installiert sind (s. Kasten „Was sind Pipes?“). Sollten solche Geräte bei ihnen nicht installiert sein, ist Ihr Rechner durch die im Folgenden beschriebenen Methoden grundsätzlich nicht aus der Ruhe zu bringen. Die erwähnten Geräte erlauben das Starten von Programmen durch einfache Übergabe des Pfadnamens an die jeweilige Pipe. Wenn Sie das AWNPipe-Gerät installiert haben sollten, verwenden sie einmal testhalber folgenden Pfad als Argument für einen Shell-Befehl (beispielsweise `COPY` oder `TYPE`):

```
"AWNPipe:test/h/eDELETE ram:disk.info"
```

und sie werden feststellen, dass der Befehl `DELETE` aufgerufen und die Datei RAM:Disk.info gelöscht wird. Das klingt bisher nicht besonders aufregend, da Sie ebenso den DELETE Befehl direkt aufrufen könnten. Das besondere an obigem Beispiel ist aber, dass diese Zeichenkette nicht nur in einem Shell-Fenster funktioniert – sondern überall dort, wo die Open() Funktion der dos.library zum Einsatz kommt. Diese Funktion wird von Amiga Programmen immer dann benutzt, wenn eine Datei geöffnet werden muss.

Was sind Pipes ?

„Pipe“ ist die Abkürzung für „Pipeline“. Dieser Begriff umschreibt die Aufgabe einer Pipe recht treffend: Pipes dienen als Verbindungen, sie besitzen zwei „Öffnungen“. Ein Programm kann auf der einen Seite Daten in eine Pipe hineinschreiben, während ein anderes Programm diese Daten auf der anderen Seite in Empfang nimmt. Das kann beispielsweise in Batch-Dateien oder ARexx-Skripten sehr nützlich sein. Das Gerät PIPE: ist ein Bestandteil von AmigaOS und ist im Verzeichnis `DEVS:DOSDrivers` zu finden. Zur Klarstellung: Das normale PIPE:-Gerät des AmigaOS stellt keine Gefahr dar und kann nicht in der hier beschriebenen Weise missbraucht werden.

In der Unix Welt sind Pipes jedoch erheblich leistungsfähiger, unter anderem kann eine Pipe dort auch selbständig Programme ausführen. Im Laufe der Jahre sind mehrere Nachbauten dieser mächtigen Pipe-Geräte für das AmigaOS veröffentlicht worden. Sei es um die Portierung von Programmen aus der Unix Welt zu vereinfachen, oder um die (absolut sinnvolle) Funktionalität einer solchen Pipe auch für Amiga-Anwender verfügbar zu machen.

Von folgenden Pipe Geräten für das AmigaOS ist derzeit bekannt, dass sie in der Lage sind, selbstständig Programme auszuführen:

- AWNPipe (Bestandteil von Aweb)
- APipe (Bestandteil von AmiTCP/Genesis)
- BlaDevice (util/cli/BlaDevice10.lha)

Die Eigenschaft, selbstständig Programme ausführen zu können, macht diese Geräte unter bestimmten Voraussetzungen zu einem Sicherheitsrisiko - nicht weil sie etwa fehlerhaft sind, sondern einfach aufgrund ihres mächtigen Funktionsumfanges.

Im Klartext: Immer wenn ein Programm versucht, eine Datei zu öffnen ist es möglich, mittels speziell manipulierter Datei- bzw. Pfadnamen ein Programm ausführen zu lassen! Ein potentieller Angreifer müsste also einen Weg finden, Ihre Internet-Applikationen zum Aufruf der Open-Funktion zu „überreden“. Sobald ihm das gelingt, sind ihm (sofern Sie eines der erwähnten Pipe-Geräte installiert haben) Tür und Tor geöffnet. Dabei stehen ihm sogar mehrere Möglichkeiten offen, um eine Nutzung der Open-Funktion zu erzwingen:

- Er erstellt eine Webseite, die Bilder bzw. Hintergrundbilder enthält. Anstatt für die Bilder eine richtige URL anzugeben („http://...“), gibt er ihren Pfad mit „file:///...“ an - dadurch wird dem Web-Browser mitgeteilt, er solle die Datei von der lokalen Festplatte laden. Und schon ruft Ihr Browser die Open-Funktion auf.
- Wenn Sie Dateien aus dem Internet herunterladen, überprüft ihr Browser, ob diese Datei auf Ihrer Festplatte bereits existiert (beispielsweise um nachzufragen, ob die existierende Datei überschrieben werden soll). Dazu benutzt er ebenfalls die Funktion Open(). Auf diese Weise sind übrigens nicht nur Web-Browser angreifbar, sondern unter anderem auch IRC Clients.
- Alle Programme, die sich die graphische Oberfläche MUI zunutze machen, sind besonders gefährdet: Mittels sogenannter „Escape-Codes“ kann ein MUI Programm überall dort, wo Text angezeigt wird, die Gestaltung des Textes beeinflussen – beispielsweise um Fettdruck oder kursive Schrift einzuschalten. Auch die Einbindung von Grafiken ist auf diese Weise möglich. Sie ahnen es bestimmt schon: Eine solche Grafik wird natürlich mit der Funktion

Open() geöffnet. Hier gibt es unzählige Möglichkeiten, eine MUI-Applikation auszutricksen, ein Beispiel wäre eine entsprechend manipulierte Betreff-Zeile einer E-Mail.

Was tun?

Sollten Sie auf Nummer sicher gehen wollen, oder es gibt von bestimmten Programmen, die Sie regelmäßig nutzen, keine Version die ausdrücklich als immun gegen die beschriebenen Angriffsmöglichkeiten gilt (s. u.), interessieren Sie sich vielleicht für die „Holzhammer Methode“:

Da alle beschriebenen Angriffsmethoden die „Anwesenheit“ eines der eingangs erwähnten Pipe-Clones voraussetzen, ist das Entfernen all dieser Clones von Ihrer Festplatte die einfachste Abwehrmaßnahme - die zugleich auch einen hundertprozentigen Schutz bietet. Mehr Informationen dazu im Kasten „Weg mit den Pipes!“.

Weg mit den Pipes!?

Um auf Nummer sicher zu gehen, löschen Sie einfach die in Frage kommenden Pipe: Geräte. Beachten Sie dabei, dass ein einfaches Verschieben nach SYS:Storage/DOSDrivers/ i.d.R. nicht ausreicht, da die Geräte dort von einigen Anwendungen gefunden und dann im Bedarfsfall nachträglich angemeldet werden.

AWNPipe: Dieses Gerät wird bei der Installation von AWeb auf Ihre Festplatte kopiert, und zwar automatisch in das DEVS:DOSDrivers/ Verzeichnis. Es wird für das ARexx-Skript "news.awebrx" benötigt. Sollten Sie AWeb nicht zum Lesen von Newsgroups benutzen (oder ausschließlich den internen Newsreader verwenden), wird AWNPipe: nicht für die Nutzung von AWeb benötigt.

Da AWNPipe aber auch einige für ARexx-Programme sehr nützliche Funktionen bietet, z.B. zur Erstellung graphischer Benutzeroberflächen, gibt es einige ARexx-Skripte, die das Gerät zwingend voraussetzen. Beispiele wären die YAM Erweiterung "Yahoogroups-Scanner" oder das mit OS 3.5/3.9 mitgelieferte Commodity "T.H.E".

Um AWNPipe zu entfernen, löschen Sie die Dateien DEVS:DOSDrivers/AWNPipe und L:awnpipe-handler.

APipe: Das APIPE: Gerät wird von verschiedenen Server-Diensten (FTP Daemon, Finger Daemon) benutzt, die mit AmiTCP/Genesis installiert werden. Es wird jedoch (zumindest bei neueren Versionen) nicht mehr automatisch in das Verzeichnis DEVS:DOSDrivers/ installiert.

Die Wahrscheinlichkeit, dass Sie dieses Gerät benötigen, dürfte relativ gering sein. Wenn Sie es entfernen möchten, löschen Sie die Dateien AmiTCP:l/apipe-handler und AmiTCP:devs/apipe-mountlist.

BLA: Kurz vor Redaktionsschluß wurde bekannt, dass dieses vom Author "BlaDevice" getaufte Gerät in dem für uns wesentlichem Punkt die gleiche Funktionalität wie APipe oder AWNPipe bietet.

Es dürfte relativ unwahrscheinlich sein, dass dieses Gerät bei ihnen installiert ist. Uns sind derzeit auch keine Anwendungen bekannt, die davon Gebrauch machen. Entfernen Sie gegebenenfalls die Dateien DEVS:DOSDrivers/BLA und L:BlaHandler von Ihrer System-Partition.

Von den oben geschilderten Beispielen hat vor allem die potentielle Lücke in MUI für hitzige Diskussionen gesorgt. Die eine Partei sieht es als Aufgabe der Programmierer an, Texte zu überprüfen,

bevor sie an MUI weitergegeben werden. Daraus folgt dass alle Applikationen, die Texte aus dem Netzwerk/Internet weiterverarbeiten, diese Texte selbständig filtern sollten. Diese Sichtweise haben sich verschiedene Programmierer zu eigen gemacht, folgende Programme sind deshalb nach Angaben ihrer Entwickler durch „MUI-Tricksereien“ nicht mehr zu überlisten:

- Alle Vaporware Produkte (Voyager, AmIRC, Microdot-II etc.)
- YAM (Version 2.3p1 oder höher)
- SimpleMail
- AmigaAIM (Version 0.9437 oder höher)

Zu dieser Liste kann man noch Amster hinzufügen, da die OpenNap-Server von sich aus bereits keine Escape-Sequenzen erlauben.

Eine andere Sichtweise besagt, dass es Aufgabe von MUI sei, verdächtige Pfadangaben auszufiltern und es sich hier um eine Sicherheitslücke in MUI handelt. Jörg Strohmayer (PINT, SFS) hat auf seiner Homepage einen Patch für MUI veröffentlicht, der die muilowlevel.library entsprechend anpasst. Es handelt sich hier um einen inoffiziellen Patch, die MUI Entwickler selbst haben sich zu dem Thema nicht öffentlich geäußert.

Offensichtlich immer noch anfällig gegen Escape-Sequenzen (sofern der erwähnte MUI-Patch nicht installiert wurde) sind folgende Programme:

- IBrowse (ein Fix ist für die kommende Version 2.3 angekündigt)
- StrICQ
- PINT (Jörg Strohmeyer verweist auf seinen MUI-Patch)
- ältere Versionen von AmigaAIM und YAM

Gegen die anderen beschriebenen Angriffsmöglichkeiten muß der Anwendungs-Programmierer vorgehen, indem er gezielt alle anfallenden Dateinamen bzw. Dateiverweise prüft. Vaporware gibt an, dass alle ihre Applikationen schon seit längerem auch gegen diese Angriffe gewappnet sind. Allerdings konnte Jörg Strohmeyer nachweisen, dass die von Vaporware verwendete Prüfmethode zumindest noch Zugriffe auf das BlaDevice zuläßt (dass dieses ebenfalls das Starten von Programmen ermöglicht, wurde erst kurz vor Redaktionsschluss bekannt). Von den AWeb-Machern war leider nicht mehr rechtzeitig eine Stellungnahme zu bekommen, laut Jörg Strohmayer scheint AWeb jedoch alle Angriffe erfolgreich abzublocken - ebenso wie SimpleHTML. Für IBrowse ist auch hier ein Fix für die kommende Version angekündigt.

Als zumindest potentiell angreifbar müssen also derzeit folgende Anwendungen gelten (Zusätzlich zu den bereits oben erwähnten):

- Voyager (nur Zugriffe auf das BlaDevice möglich, s.o.)
- IBrowse (Fix für die kommende Version angekündigt)

Wir bemühen uns um Stellungnahmen weiterer Entwickler, und werden diese gegebenenfalls nachreichen.