Robert Lemos, News.com, 2004.12.01:

“Microsoft rushes out critical IE fix

“Microsoft published a patch for Internet Explorer on Wednesday, aiming to close a month-old hole that has been used by viruses to spread and by an ad banner attack to compromise PCs.

“The vulnerability, dubbed the Internet Explorer Elements flaw by Microsoft, had previously been called the iFrame vulnerability. . . .

“A Microsoft representative said the software giant had released the update before its next scheduled patch day, Dec. 7, because it had already been used

by malicious software to compromise Windows users' PCs. . . .

"An attacker can use the vulnerability to gain control of a person's computer when the victim clicks on a simple Web link. The attacker would then have complete control of the system . . .

"The patch arrived more than a month after news of the vulnerability was first posted on public security mailing lists. The move garnered criticism from Microsoft, which has led a drive to convince security researchers to give software makers at least 30 days to fix issues before outing the problem in public forums."

Next week:

Monday office hours 14:00–17:00.

Wednesday office hours 14:00–17:00.

Thursday final exam 08:00–10:00.

Writer merges information from
several sources into one stream;
e.g., merges many mail messages
into a single mbox file.

Reader parses the stream to
extract one piece of information;
e.g., reader parses mbox file
to extract one mail message.

Common security hole:
Merge and parse don't exactly match,
so one source of information can
corrupt data from another source.

Mixed-source HTTP data

Browser can request
more than one page from server:
make TCP connection,
send URL of first page,
read first page,
send URL of second page,
read second page, etc.

Where does each page end?
A little more complicated
than the mbox answer.

General problem announced
2004.03.04 by Amit Klein
(“HTTP response splitting”):
Many servers allow attacker
to insert a fake page
by including a page-end.

Browser then trusts fake page;
also saves it for later.

See, e.g., phpWebSite
security hole fixed 2004.11.16.

Mixed-source command lines

Pine bug fixed 2002.01.09:

```
url_launch(...)
{
  ...
  if (...) return too_long;
  sstrcpy(&cmdp,browser);
  sstrcpy(&cmdp," '");
  sstrcpy(&cmdp,url);
  sstrcpy(&cmdp,"'");
  system(cmdp);
  ...
}
```

Impact: If attacker sends you a URL, and you click on the URL in Pine, attacker can take over your account.

`system("foo bar")` calls

```
execv("/bin/sh",
  {"sh","-c","foo bar",0})
```

which has same effect as
typing `foo bar` in shell.

`/bin/sh` parses `foo bar`
in a complicated way.
Ends up calling

```
execvp("foo",{"foo","bar",0})
```

because space is special.
(`execvp` tries `execv` using
`/bin/foo`, `/usr/bin/foo`, etc.;
see `$PATH` environment variable.)

Many special characters:
`$&'()*;<>?[]{|}~` and others.

Say user's browser is `konqueror`,
URL is `cnn.com`.

Pine builds string

```
konqueror 'cnn.com'
```

and then `system` calls

```
execv("/bin/sh",
  {"sh","-c",
  "konqueror 'cnn.com'",0})
```

and then `/bin/sh` calls

```
execvp("konqueror",
  {"konqueror","cnn.com",0})
```

and then `konqueror` views `cnn.com`.

(Why doesn't Pine run `konqueror`
directly, without using `sh`?
Good question.)

What do the quotes do?

Pine programmer was thinking:
Any string between single quotes
is passed along as an argument,
even if it has special characters.

e.g. `konqueror 'cnn;rm x'` calls

```
execvp("konqueror",
  {"konqueror","cnn;rm x",0})
```

so `konqueror` views the URL `"cnn;rm x"`.

`konqueror cnn;rm x` would have
run `konqueror cnn` and then
run `rm x`, removing file `x`.
Semicolons are special.

The programmer put one string
between one pair of quotes.

When the shell sees a quote,
it looks for the next quote.

These are not inverse operations!

If the URL is

```
cnn.com';rm x'
```

then Pine runs

```
konqueror 'cnn.com';rm x''
```

which removes `x`.

Common mistake. See, e.g.,
licq bug fixed 2001.03.13.

Mixed-source SQL queries

`mod_auth_pgsql` provides
limited network access to a database.

`mod_auth_pgsql` bug fixed 2001.10:

```
Query := Sprintf
  ("SELECT %s FROM %s
    WHERE %s = '%s'",
   Password_Column, User_Table,
   User_Column, User);
```

with `User` taken from attacker.
Just like the Pine bug.

Impact: Typically, attacker obtains
complete control over the database.

Two more Sendmail bugs

Bug fixed 1996.01.25:
"In some cases it was still possible
for an attacker to insert newlines
into a queue file, thus allowing
access to any user (except root)."

Queue file has many lines.
Lines starting with C et al. are
trusted to specify uid for deliveries.
Lines starting with H et al. are
from message sender.

Attacker could insert newline
and then a trusted line specifying uid.

Recall that `/home/djb/.forward`
can specify program to run for
each incoming message to `djb`.
Queue file: `R|prog`.

Queue file also has recipient addresses:
`Rjoe`, `Rbill@aol.com`, etc.

Bug fixed 1993.10.31:
When Sendmail returned a message
to the sender, it copied the
sender's address to `R` line
in the return-message queue file.

Doesn't exactly match the parsing:
sender's address may be `|rm *`.

Chris Strohm, GovExec, 2004.12.01:

“Tenet warns of terrorists combining physical, telecommunications attacks

“Former CIA Director George Tenet on Wednesday said greater government regulation of the Internet and telecommunications networks is needed in order to guard against terrorist attacks.

“The U.S. intelligence community needs to consider how terrorists might attempt to couple an attack on telecommunication networks with a physical attack, Tenet said during a keynote speech at the E-Gov Institute’s homeland security conference in Washington. . . .

“ ‘The number of known potential adversaries conducting research on information attacks is increasing rapidly and includes intelligence services, military organizations and nonstate entities.’ . . .

“Telecommunications technology for government and business should have built-in protections, Tenet said, such as intrusion detection and protection systems, antivirus software, authentication and identify management services, and encryption.

“ ‘I know that these actions would be controversial in this age where we still think the Internet is a free and open society with no control or accountability,’

he added. ‘But, ultimately, the Wild West must give way to governance and control.’

“Many national media outlets were not allowed to attend Tenet’s speech. The Associated Press reported that Tenet insisted that national media be kept out, only allowing in reporters for trade publications that cover the government.”