ITS Technical Notes

Iowa State University
Windows Enterprise Announcement

April 3, 2007 – Important Zero-Day Vulnerabilty Security Update

Microsoft released a security update **today** for a “zero-day vulnerability”. Microsoft is taking this vulnerability very seriously and issuing a rare "out of band" security update. The vulnerability involves ".ani" files. These are files that define animated cursors. It is possible to embed code in malformed ani files to take control of a system.

Microsoft has issued "Microsoft Security Bulletin MS07-017". It addresses a number of problems with the GDI and discusses the animated cursor problems as well. You can read MS07-017 at:

http://www.microsoft.com/technet/security/Bulletin/MS07-017.mspx

Make sure that your systems receive this new security update. The update was received and approved for installation on the Enterprise WSUS server early this afternoon.

Other Information

SANS reports that hacker tool kits for building malformed ani files have been distributed widely among the hacker community. See the SANS Diary for details and some very good links on the topic:

http://isc.sans.org/diary.html?storyid=2551

The most detailed analysis of the problem to date is reported in a CERT advisory:

http://www.kb.cert.org/vuls/id/191609