Die Warnowregion wird aktiv!

e-mail: mail@warnowregion.de Internet: www.warnowregion.de www.baltcoast.org

Warnow-Neuigkeiten Nr. 03/2007

- Sonderausgabe -

vom 04.04.07

Alarmierende Sicherheitswarnungen seriöser Informationsanbieter - offenbar kein Aprilscherz!

1. Der Europaticker-Umweltruf meldete am 4.4. in einer Extra-Email:

Dringende Warnung: Pfeilangriff auf Windows

Lesen Sie E-Mails nur im Klartext-Format

> Wie das Bürger-CERT bereits berichtet, existiert zur Zeit eine kritische Sicherheitslücke in Microsoft Windows bei der Verarbeitung von Dateien zur Darstellung des Mauszeigers (.ani). Die Schwachstelle ermöglicht es unter Windows, Schadprogramme auf den Computer einzuschleusen. Dazu reicht bereits allein das Betrachten einer manipulierten Webseite oder einer bösartigen E-Mail aus. Besonders problematisch daran ist, dass .ani-Dateien u.a. auch als Bilddateien (z.B. JPG) getarnt werden können.

Bitte beachten Sie ...

... dass die Redaktion Europaticker derzeit keine Pressemitteilungen, die nicht im Klartext versandt werden, öffnet.

Das Bürger-CERT stellt zur Zeit fest, dass die Schwachstelle massiv über manipulierte Webseiten ausgenutzt wird. Derzeit bestehen nur wenige Möglichkeiten, sich vor Angriffen zu schützen. Das Risiko kann jedoch durch folgende Massnahmen verringert werden:

- Melden Sie sich an Ihrem System nur mit eingeschränkten Benutzerrechten und nicht als Administrator an.
- Lesen Sie E-Mails nur im Klartext-Format.
- Besuchen Sie zudem nur Ihnen vertraute Webseiten und folgen Sie keinen Links in E-Mails.
- Halten Sie Ihren Virenscanner immer aktuell.

Microsoft hat angekündigt am Dienstag, den 3. April, ein Sicherheitsupdate zu veröffentlichen, das die Schwachstelle behebt. Achten Sie daher auf Meldungen von Microsoft und installieren Sie das Sicherheitsupdate umgehend nach Veröffentlichung.

erschienen am: 2007-04-04 im Umweltticker

2. Der Heise-online-Newsticker (www.heise.de) meldet hierzu:

Vorgezogenes Update von Microsoft für ANI-Lücke

Microsoft[1] hat wie angekündigt[2]

einen vorgezogenen Patch für die kritische Sicherheitslücke[3] bei der Verarbeitung präparierter Dateien für animierte Cursor (.ani) in zahlreichen Windows-Versionen herausgegeben.Damit schließt der Redmonder Konzern die bereits aktiv ausgenutzte Schwachstelle eine Woche vor dem offiziellen Patchday. Das Update behebt aber auch noch weitere Sicherheitslöcher. Die gravierendste Lücke, die das Update schließt, ist die von Determina entdeckte und bereits im Dezember 2006 an Microsoft gemeldete Schwachstelle beim Verarbeiten von defekten Dateien für animierte Cursor. Sie betrifft die Systembibliothek USER32.DLL der Betriebssysteme Windows NT, 2000, XP, 2003 und auch in Windows Vista...

[Es sollten alle Windows-]Anwender das Update von Microsoft, das die Lücke schließt, so schnell wie möglich einspielen. Etwaige inoffizielle Patches von Drittanbietern sollte man allerdings vorher deinstallieren.

Das Update zu Microsofts Security Bulletin MS07-017 schließt noch weitere Lücken, durch die Angreifer und lokale Nutzer ihre Rechte ausweiten oder das System zum Absturz bringen konnten. Dies konnte unter anderem durch manipulierte WMF- und EMF-Grafiken geschehen. Außerdem enthielt die Render-Engine GDI mehrere Lücken, durch die Anwender oder bösartige Anwendungen ihre Rechte erhöhen und so die komplette Kontrolle über ein System übernehmen konnten. Diese Lücken stuft Microsoft jedoch allesamt lediglich als "wichtig" oder "moderat"ein, nur der Fehler beim Verarbeiten manipulierter animierter Cursor erhält den Status "*kritisch*".

Microsoft äußerte sich noch nicht dazu, ob am eigentlichen Patchday-Termin am Dienstag kommender Woche weitere Updates veröffentlicht werden. Immerhin listen einige Sicherheitsdienstleister noch mehrere kritische[5] Sicherheitslücken in Microsoft-Produkten auf, für die es bislang noch keine Patches gibt.

Siehe dazu auch:

Vulnerabilities in GDI Could Allow Remote Code Execution[6], Sicherheitsmeldung von Microsoft
Windows Animated Cursor Stack Overflow Vulnerability[7], detaillierte Sicherheitsmeldung zur ANI-Schwachstelle von Determina

(dmk[8]/c't)

URL dieses Artikels:
http://www.heise.de/newsticker/meldung/87829

Links in diesem Artikel:
[1] http://www.microsoft.de/
[2] http://www.heise.de/security/news/meldung/87724
[3] http://www.heise.de/newsticker/meldung/87633
[4] http://www.heise.de/security/news/meldung/55138
[5] http://www.heise.de/security/news/meldung/87821
[6] http://www.microsoft.com/technet/security/Bulletin/MS07-017.mspx
[7] http://www.determina.com/security.research/vulnerabilities/ani-header.html
[8] mailto:dmk@ct.heise.de

Die „Warnow-Neuigkeiten“ werden im Auftrag des Vereins Warnowregion e.V. vom Büro Warnowprojekt der OIKOS GmbH herausgegeben.

Sie gehen allen Verwaltungsämtern zu, die vollständig (mit allen Gemeinden) oder anteilig (mit einigen ihrer Gemeinden) in der Warnowregion liegen, ebenso den Landkreisen und Fachämtern und den Lokalredaktionen der Tageszeitungen. Sie erscheinen auf der Internetseite www.warnowregion.de und können darüber hinaus von allen Interessenten als email abonniert werden (Bestellungen wie auch Abbestellungen bitte formlos unter mail@warnowregion.de). Eine Zustellung per Post oder als Fax ist aus Kostengründen leider nicht möglich.

Wir freuen uns, wenn Informationen aus den „Warnow-Neuigkeiten“ in die Kreis- und Amtsblätter und von der Presse übernommen werden. Ebenso freuen wir uns über Zuarbeiten zur Veröffentlichung.

Die Amtsverwaltungen bitten wir, die „Warnow-Neuigkeiten“ an ihre amtszugehörigen Gemeinden und gegebenenfalls an interessierte Vereine, Betriebe und Bürger weiterzugeben.

Redaktion: Dr. Günter Hering, Rodompweg 11, 18146 Rostock. Tel.: 0381/8003935, email: mail@warnowregion.de