

Alaska Computer Society PC User Group - <http://www.acs-pcug.org/>

PC Security snapshot – March 2006

SANS (SysAdmin, Audit, Network, Security) Institute Newsletters

<http://www.sans.org/aboutsans.php>

<http://www.sans.org/newsletters/>

Ouch! – End Users newsletter

<http://www.sans.org/newsletters/ouch/issue/20060307.php>

@ RISK - Security Vulnerability Alerts – Weekly newsletter

<http://www.sans.org/newsletters/risk/display.php?v=5&i=9>

March 6, 2006 Vol. 5. Week 9

Apple patched several critical vulnerabilities in its Safari browser and fixed other security problems in Mac OS X. And Oracle is recommending its new patch be applied now.

@RISK is the SANS community's consensus bulletin summarizing the most important vulnerabilities and exploits identified during the past week and providing guidance on appropriate actions to protect your systems

Summary of the vulnerabilities reported this week:

=====

Platform	# of Updates & Vulnerabilities
----------	--------------------------------

=====

Other Microsoft Products	1
Third Party Windows Apps	11
Mac Os	1 (Critical)
Linux	7
BSD	1
Solaris	1
Unix	1
Cross Platform	14
Web Application - Cross Site Scripting	16
Web Application - SQL Injection	14
Web Application	21
Network Device	4

Widely Deployed Software

(1) CRITICAL: Apple Cumulative Security Update 2006-001

Affected:

Mac OS X version 10.3.9 and 10.4.5 (including the server)

Description: Apple has released a cumulative security update for Mac OSX that fixes 20 vulnerabilities. This update fixes several critical vulnerabilities in Safari browser that can be exploited by a malicious

webpage to compromise a user's system. Exploit code for one of the Safari flaws is publicly available and was discussed in the last week's @RISK newsletter. This security update also fixes code execution vulnerabilities in LibSystem, WebKit and rsync components. Apple also made security enhancements to warn iChat users attempting to download unsafe file types to prevent worms like Leap.A.

Status: Apply the Mac OS X security update 2006-001 on a priority basis.

Council Site Actions: Two of the reporting council sites are using the affected software. One site will be distributing the patches during their next regularly scheduled system update process. The other site uses Apples Software Update Facility and hence most of their systems are already patched or will be soon.

References:

Apple Security Advisory

<http://docs.info.apple.com/article.html?artnum=303382>

Internet Storm Center Articles on this set of problems/solutions:

<http://isc.sans.org/diary.php?storyid=1160>

<http://isc.sans.org/diary.php?storyid=1145>

<http://isc.sans.org/diary.php?storyid=1138>

<http://isc.sans.org/diary.php?storyid=1128>

iDefense Advisory

<http://archives.neohapsis.com/archives/vulnwatch/2006-q1/0074.html>

Suresec Advisories

<http://www.suresec.org/advisories/adv10.pdf>

<http://www.suresec.org/advisories/adv11.pdf>

SANS Handler's Diary Postings

<http://isc.sans.org/diary.php?storyid=1160>

<http://isc.sans.org/diary.php?storyid=1145>

<http://isc.sans.org/diary.php?storyid=1138>

<http://isc.sans.org/diary.php?storyid=1128>

Previous @RISK Newsletter Posting

<http://www.sans.org/newsletters/risk/display.php?v=5&i=8#widely1>

Leap.A virus

<http://www.sophos.com/virusinfo/analyses/osxleapa.html>

SecurityFocus BID

<http://www.securityfocus.com/bid/16907>

Apple Security Updates:

- Resource page

<http://docs.info.apple.com/article.html?artnum=61798>

<http://docs.info.apple.com/article.html?artnum=303382>

Microsoft Security updates - Patch Tuesday;

Next Scheduled Release: March 14, 2006

Microsoft Anti-spyware – Defender

<http://www.microsoft.com/athome/security/spyware/software/default.aspx>

<http://www.microsoft.com/athome/security/spyware/software/msft/antispywarecycle.aspx>