

[VulnWatch] Microsoft Virtual PC Services Insecure Temporary File Creation

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2004-02/0011.html>

From: Advisories (advisories_at_atstake.com)

Date: 02/10/04

Date: Tue, 10 Feb 2004 14:34:27 -0500

To: <vulnwatch@vulnwatch.org>

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

@stake, Inc.

www.atstake.com

Security Advisory

Advisory Name: Virtual PC Services Insecure Temporary File Creation

Release Date: 02/10/2004

Application: Connectix Virtual PC 6.0.x

Microsoft Virtual PC 6.1

Platform: Mac OS X

Severity: Local privilege escalation

Author: George Gal <ggal@atstake.com>

Vendor Status: Vendor has updated version of the software

CVE Candidate: CAN-2004-0115

Reference: www.atstake.com/research/advisories/2004/a021004-1.txt

Overview:

Virtual PC is a popular x86 virtual machine emulator capable running several guest operating systems under the Mac OS X and Windows platforms. Virtual PC provides a set of services for managing network sharing capabilities under Mac OS X. These services are spawned from the `setuid` root binary, `VirtualPC_Services`, which creates several temporary files when it is executed. The `VirtualPC_Services` does not check for several unsafe conditions prior to creation of these temporary files. As a result an attacker with interactive login access to the system may leverage insecure temporary files to become root or overwrite critical system files.

Details:

@stake has identified a vulnerability within the `setuid` root binary, `VirtualPC_Services`, due to its inability to check for dangerous conditions prior to temporary file creation. This vulnerability allows an attacker to truncate and overwrite arbitrary files in addition to creation of arbitrary files with insecure file permissions.

VulnWatch: [VulnWatch] Microsoft Virtual PC Services Insecure Temporary File Creation

Using this vulnerability it is feasible for an attacker to gain root privileges on the system. The VirtualPC_Services binary creates a log file upon startup as /tmp/VPCServices_Log. An attacker may create a symbolic link in the /tmp/ directory as VPCServices_Log pointing to an arbitrary file to be overwritten when the VirtualPC_Services binary is executed. However, when the symbolic link points to a non-existent file a new file is created with file permissions determined by the unprivileged user's umask(2) settings.

Vendor Response:

Microsoft has an updated version of the software available.

Download information available at:

<http://www.microsoft.com/technet/security/bulletin/MS04-005.asp>

Recommendation:

If possible install the updated version of Virtual PC.

Do not install Virtual PC on a multi-user machine. If this is a requirement, only allow users within a particular group to access Virtual PC.

Common Vulnerabilities and Exposures (CVE) Information:

The Common Vulnerabilities and Exposures (CVE) project has assigned the following names to these issues. These are candidates for inclusion in the CVE list (<http://cve.mitre.org>), which standardizes names for security problems.

CAN-2004-0115

@stake Vulnerability Reporting Policy:

<http://www.atstake.com/research/policy/>

@stake Advisory Archive:

<http://www.atstake.com/research/advisories/>

PGP Key:

http://www.atstake.com/research/pgp_key.asc

Copyright 2004 @stake, Inc. All rights reserved.

-----BEGIN PGP SIGNATURE-----

Version: PGP 8.0.3

iQA/AwUBQCKrWke9kNifAm4yEQJr3gCgzh/grlYI0dPRnvOmCYIYXPtTKTEAniMG

FMuE/Uyj9h/1q8+peD80BmPq

=W/J8

-----END PGP SIGNATURE-----