

[NT] Windows 2000 Weak Default Permission on System Partitions

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-08/0019.html>

From: support@securiteam.com

Date: 08/07/02

From: support@securiteam.com

To: list@securiteam.com

Date: Wed, 7 Aug 2002 23:43:37 +0200 (CEST)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Windows 2000 Weak Default Permission on System Partitions

SUMMARY

The system partition by default has Everyone/Full Control access permission. Further, Microsoft's (and NIST draft) documents recommend the permission settings of Everyone/Full Control or Authenticated Users/Full Control is given to the system partition. Of course, these kinds of permissions settings are inertly weak and would allow both a remote and local attacker to gain elevated privileges.

DETAILS

Introduction:

To protect any system files located in the root of system partition (boot.ini, ntdetect.com, NTLDR, autoexec.bat etc), Windows 2000 applies a security template with the NTFS permissions that allow only administrators and advanced users to access these files.

Details:

In order to provide POSIX compatibility, users will be provided with Full Control NTFS permissions for all the folders. This allows them to delete any file regardless of its individual file permission. This would allow a user to become the owner of any file and to further gain full control to

Securiteam: [NT] Windows 2000 Weak Default Permission on System Partitions

any system file located in root of system partition. The following scenario is possible:

1. Delete original file (only delete, because putting file into recycle bin requires read permission).
2. Create new file with the same name. Make the user, the owner for this new file giving him Full Control permissions for this file (as it is inherited from root folder).

This means a user can Trojan a system files causing it to execute some arbitrary code inside the kernel space and/or to change boot sequence.

Solution:

Replace the Full Control permission settings given to the group Everyone with any reasonable set of permissions.

ADDITIONAL INFORMATION

The information has been provided by <mailto:3APA3A@security.nnov.ru>
ZARAZA.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

-
- **Previous message:** [list-unsubscribe: "DEFER LANGUAGE"](#)
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)