

03/01/2023

Security Bulletin

Microsoft Security Bulletin MS99-008 - Critical

Patch Available for Windows NT "Screen Saver" Vulnerability

Published: March 12, 1999 | Updated: March 10, 2003

Version: 2.0

Patch Availability Information Updated: March 10, 2003

Originally Posted: March 12, 1999

Summary

Microsoft has learned of a vulnerability affecting all versions of Microsoft® Windows NT® operating system, which could allow a user to gain administrative privileges on a computer. In most common usage scenarios, this vulnerability presents itself on workstations, terminal servers, and other systems that allow non-administrative users to interactively log on. Less-common configurations could also be affected, and are discussed below.

A fully supported patch is available to eliminate the vulnerability, and Microsoft recommends that affected customers download and install it, if appropriate.

Issue

Windows NT provides a screen saver feature, in which a user-selected screen saver program is run when the machine has been idle for a specified length of time. Windows NT initially launches a screen saver in the local system context, then immediately changes its security context to match that of the user. However, Windows NT does not check whether this context change was successfully made. This is the underlying problem in this vulnerability. If the context change can be made to fail, the screen saver will remain running in a highly-privileged state. The risk is that a malicious user could develop a screen saver program that, for example, uses the elevated privileges to add the author to the Administrators group.

IPR2025-01468; Citrix

Ex. 1020 - Page 1

It is important to understand that the user must be able to run exploitation code on a machine in order to elevate their privileges. There are two types of machines at risk:

- Machines that allow non-administrative users to interactively log on. Workstation and terminal servers typically do allow this, but, per standard security practices, most other machines only allow administrators to interactively log on.
- Machines that allow remote users to submit arbitrary programs for execution. Servers such as domain controllers, line of business servers, application servers, print and file servers and the like typically do not accept arbitrary programs for execution.

It also is important to note that the scope of the privilege elevation is highly dependent on the specific machine on which the exploitation code is run. For example, a user who exploited this vulnerability on a workstation could join the local Administrators group, but could not directly exploit this vulnerability to become a domain administrator. However, a user who exploited this vulnerability on a domain controller would be able to become a domain Administrator, because the domain SAM is shared among all domain controllers.

While there are no reports of customers being adversely affected by this vulnerability, Microsoft is proactively providing a patch to allow customers to take appropriate action to protect themselves against it.

Affected Software Versions

- Microsoft Windows NT Workstation 4.0
- Microsoft Windows NT Server 4.0
- Microsoft Windows NT Server 4.0, Enterprise Edition
- Microsoft Windows NT Server 4.0, Terminal Server Edition

Vulnerability Identifier: [CVE-1999-0382](#) 

What Microsoft is Doing

Microsoft has released patches that fix the problem identified. The patches are available for download from the sites listed below in *What Customers Should Do*.

Microsoft also has sent this security bulletin to customers subscribing to the Microsoft Product Security Notification Service. See [The Microsoft Product Security Notification Service](#)  for more information about this free customer service.

Microsoft has published the following Knowledge Base (KB) article on this issue:

IPR2025-01468; Citrix

Ex. 1020 - Page 2

- Microsoft Knowledge Base (KB) article 221991, [Screen Saver Vulnerability Lets User Privileges be Elevated](#) [↗](#).
(**Note** It might take 24 hours from the original posting of this bulletin for the KB article to be visible in the Web-based Knowledge Base.)

What customers should do

Microsoft highly recommends that customers evaluate the degree of risk that this vulnerability poses to their systems and determine whether to download and install the patch. The patch can be found at:

- X86-based Windows NT Workstation and Server 4.0 (including Enterprise Edition):
<https://www.microsoft.com/technet/security/patchavailability.mspix> [↗](#)
- X86-based Windows NT Server 4.0, Terminal Server Edition:
<https://www.microsoft.com/technet/security/patchavailability.mspix> [↗](#)
- Alpha-based Windows NT Workstation and Server 4.0 (including Enterprise Edition):
<https://www.microsoft.com/technet/security/patchavailability.mspix> [↗](#)
- Alpha-based Windows NT Server 4.0, Terminal Server Edition:
<https://www.microsoft.com/technet/security/patchavailability.mspix> [↗](#)

(**Note** Patches for Windows NT Server 4.0, Terminal Server Edition, will not be available immediately upon release of this bulletin, but will be released shortly after.)

More Information

Please see the following references for more information related to this issue.

- Microsoft Security Bulletin MS99-008, *Patch Available for Windows NT 'Screen Saver' Vulnerability* (the Web-posted version of this bulletin),
<https://www.microsoft.com/technet/security/bulletin/ms99-008.mspix> [↗](#) .
- Microsoft Knowledge Base (KB) article 221991, [Screen Saver Vulnerability Lets User Privileges be Elevated](#) [↗](#).

(**Note** It might take 24 hours from the original posting of this bulletin for the KB article to be visible in the Web-based Knowledge Base.)

Obtaining Support on this Issue

If you require technical assistance with this issue, please contact Microsoft Technical Support. For information on contacting Microsoft Technical Support, please see <https://support.microsoft.com/contactussupport/?ws=support> [↗](#) .

Acknowledgments

IPR2025-01468; Citrix
Ex. 1020 - Page 3

Microsoft acknowledges Cybermedia Software Private Limited for reporting this vulnerability.

Revisions

- March 12, 1999: Bulletin Created
- V2.0 (March 10, 2003): Introduced versioning and updated patch availability information

For additional security-related information about Microsoft products, please visit

<https://www.microsoft.com/technet/security> 

THE INFORMATION PROVIDED IN THE MICROSOFT KNOWLEDGE BASE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. MICROSOFT DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL MICROSOFT CORPORATION OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF MICROSOFT CORPORATION OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES SO THE FOREGOING LIMITATION MAY NOT APPLY.

Built at 2014-04-18T13:49:36Z-07:00