TOP
What's New
Notifications
Alert
Software Vulnerability Information
Links to Security Organizations
Email
soft-security@itg.hitachi.co.jp

Before sending an email, you need to read Privacy Notice and to give your consent to the contents. If you do not give your consent, you may not be able to utilize the services prescribed under the purposes of use in Privacy Notice. Only send an email to this address if you are willing to give your consent upon carefully reading Privacy Notice.
Note that personal information that is sent to this address will be erased as soon as the response to your inquiry is given, and that the Company will not retain the personal information.

Product names of Hitachi and other manufacturers

HIRT Hitachi Incident Response Team

Update: July 20, 2005

Vulnerability to Buffer Overflow in the GDIPlus function in JP1/AppManager

- Affected products

Corrective action	Product name	Platform	Last update
HS05-013-01	JP1/AppManager	Windows	July 20, 2005

- Problem description

Details about the vulnerability of the GDIPlus function in AppManager(*1) have been announced on the NetIQ Corporation website.
Malicious remote users can exploit the vulnerability of buffer overflow and execute arbitrary commands on the product mentioned above.

(*1) This announcement is titled "`What is NetIQ's recommendation with regards to the GDIPlus.DLL (GDI+) vulnerability in AppManager?`". This announcement can be referenced by searching the NetIQ Knowledge Base for the string `NETIQKB43147`.

Revision history

- July 20, 2005: This page is released.

- Hitachi, Ltd. (hereinafter referred to as "Hitachi") tries to provide accurate information about security countermeasures. However, since information about security problems constantly changes, the contents of these Web pages are subject to change without prior notice. When referencing information, please confirm that you are referencing the latest information.
- The Web pages include information about products that are developed by non-Hitachi software developers. Vulnerability information about those products is based on the information provided or disclosed by those developers. Although Hitachi is careful about the accuracy and completeness of this information, the contents of the Web pages may change depending on the changes made by the developers.
- The Web pages are intended to provide vulnerability information only, and Hitachi shall not have any legal responsibility for the information contained in them. Hitachi shall not be liable for any consequences arising out of or in

connection with the security countermeasures or other actions that you will take or have taken (or not taken) by yourself.

- The links to other web sites are valid at the time of the release of the page. Although Hitachi makes an effort to maintain the links, Hitachi cannot guarantee their permanent availability.

Page Top

Update: July 20, 2005

HS05-013;
Vulnerability to Buffer Overflow in the GDIPlus function in JP1/AppManager

Solution for JP1/AppManager

The following vulnerability was found in JP1/AppManager.
Malicious remote users can exploit the vulnerability of buffer overflow and execute arbitrary commands.
An appropriate patch for the vulnerability is available below. Please apply the patch in your system.

[Influence]

Check the version number of GDIPlus.dll in the properties file under the following path:
<installation-folder-for-JP1/AppManager>\AppManager\bin
If the version number is earlier than 5.1.3102.1355, this problem applies to your system(*1).

(*1)If the version number is 5.1.3102.1355 or later, this problem does not apply to your system.

[Affected models and versions]

Product name	Model	Version	Platform	Last update
JP1/AppManager	P-242C-3*74 (*2)	07-10	Windows	July 20, 2005
		07-11 - 07-11-/B		July 20, 2005
	P-F242C-3F74*, P-F242C-3G74* (*3)	07-10		July 20, 2005
		07-11 - 07-11-/B		July 20, 2005

(*2) "*" is a placeholder for A to E. For details, see [Detailed affected models and versions].

(*3) "*" is a placeholder for 1 to 9 or A to J. For details, see [Detailed affected models and versions].

[Detailed affected models and versions]

Product name	Model	Version
JP1/AppManager Operator Console	P-242C-3A74	
JP1/AppManager Developer Console	P-242C-3B74	

TOP
What's New
Notifications
Alert
Software Vulnerability Information
Links to Security Organizations
Email
soft-security@itg.hitachi.co.jp

Before sending an email, you need to read Privacy Notice and to give your consent to the contents. If you do not give your consent, you may not be able to utilize the services prescribed under the purposes of use in Privacy Notice. Only send an email to this address if you are willing to give your consent upon carefully reading Privacy Notice.
Note that personal information that is sent to this address will be erased as soon as the response to your inquiry is given, and that the Company will not retain the personal information.

Product names of Hitachi and other manufacturers

HIRT Hitachi Incident Response Team

JP1/AppManager for Microsoft® Windows® 2000 and Windows® XP Professional	P-242C-3D74	07-10, 07-11 - 07-11-/B	
JP1/AppManager for Microsoft® Windows NT® and Windows® 2000 Server and Windows Server™ 2003	P-242C-3E74		
JP1/AppManager for Microsoft® Windows® 2000 Advanced Server and Windows Server™ 2003 Enterprise Edition	P-F242C-3F741		
JP1/AppManager for Microsoft® Windows® 2000 Datacenter Server and Windows Server™ 2003 Datacenter Edition	P-F242C-3F742		
JP1/AppManager for Microsoft® Active Directory™	P-F242C-3F743		
JP1/AppManager for Microsoft® Cluster Service	P-F242C-3F744		
JP1/AppManager for Microsoft® Terminal Service	P-F242C-3F745		
JP1/AppManager for Microsoft® Load Balancing Service	P-F242C-3F746		
JP1/AppManager for Citrix MetaFrame XP	P-F242C-3F747		
JP1/AppManager for Microsoft® Exchange Server	P-F242C-3F748		
JP1/AppManager for Lotus Notes® and Domino™	P-F242C-3F749		
JP1/AppManager for Microsoft® Message Queue Server	P-F242C-3F74A		
JP1/AppManager for Microsoft® BizTalk™ Server	P-F242C-3F74B		
JP1/AppManager for IBM® MQSeries®	P-F242C-3F74C		
JP1/AppManager for Microsoft® Internet Information Server	P-F242C-3F74D		
JP1/AppManager for Microsoft® Internet Information Security and Acceleration Server	P-F242C-3F74E		
JP1/AppManager for IBM® WebSphere Application Server	P-F242C-3F74F		
JP1/AppManager for Microsoft® SQL Server	P-F242C-3F74G		
JP1/AppManager for Oracle® RDBMS	P-F242C-3F74H		
JP1/AppManager for Microsoft® Transaction Server	P-F242C-3F74J		
JP1/AppManager for Compaq Insight Manager®	P-F242C-3G741		
JP1/AppManager for Dell OpenManage	P-F242C-3G742		
JP1/AppManager HP TopTools for Servers	P-F242C-3G743		
JP1/AppManager for IBM® Netfinity Manager™	P-F242C-3G744		
JP1/AppManager for IBM® Director	P-F242C-3G745		
JP1/AppManager for Computer Associates ARCserve® IT™	P-F242C-3G746		
JP1/AppManager for Check Point™ FireWall-1®	P-F242C-3G747		
JP1/AppManager for Microsoft® Application Center 2000	P-F242C-3G748		
JP1/AppManager for Network Associates NetShield®	P-F242C-3G749		
JP1/AppManager for VERITAS Backup Exec™	P-F242C-3G74A		
JP1/AppManager Response Time Module for Microsoft® Exchange (10 Client Pack)	P-F242C-3G74B		
JP1/AppManager Response Time Module for Lotus Domino™ (10 Client Pack)	P-F242C-3G74C		
JP1/AppManager Response Time Module for Microsoft® SQL Server (10 Client Pack)	P-F242C-3G74D		
JP1/AppManager Response Time Module for Active Directory™ (10 Client Pack)	P-F242C-3G74E		
JP1/AppManager Response Time Module for Oracle® RDBMS (10 Client Pack)	P-F242C-3G74F		
JP1/AppManager Response Time Module for Web	P-F242C-3G74G		

JP1/AppManager Response Time Module for Network	P-F242C-3G74H	

For the fixed versions, fixed patch, and patch application procedure, contact your Hitachi support service representative.

Revision history

- July 20, 2005: Information about the vulnerability to Buffer Overflow in the GDIPlus function in JP1/AppManager is released.

- Hitachi, Ltd. (hereinafter referred to as "Hitachi") tries to provide accurate information about security countermeasures. However, since information about security problems constantly changes, the contents of these Web pages are subject to change without prior notice. When referencing information, please confirm that you are referencing the latest information.
- The Web pages include information about products that are developed by non-Hitachi software developers. Vulnerability information about those products is based on the information provided or disclosed by those developers. Although Hitachi is careful about the accuracy and completeness of this information, the contents of the Web pages may change depending on the changes made by the developers.
- The Web pages are intended to provide vulnerability information only, and Hitachi shall not have any legal responsibility for the information contained in them. Hitachi shall not be liable for any consequences arising out of or in connection with the security countermeasures or other actions that you will take or have taken (or not taken) by yourself.
- The links to other web sites are valid at the time of the release of the page. Although Hitachi makes an effort to maintain the links, Hitachi cannot guarantee their permanent availability.

Page Top