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: December 21, 2006

Multiple Vulnerabilities of the LDAP Server

- Affected products

Corrective action	Product name	Platform	Last update
HS06-018-01	Hitachi Directory Server Version 2	Windows, HP-UX	December 21, 2006

- Problem description

Multiple vulnerabilities caused by invalid LDAP requests were found in the above product.
Malicious remote users can exploit these vulnerabilities, cause DoS, and execute arbitrary code.

Revision history

- December 21, 2006: This page is released.

their permanent availability.

Page Top

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: December 21, 2006

HS06-018;
Multiple Vulnerabilities of the LDAP Server

Solutions for Hitachi Directory Server Version 2

The following vulnerabilities caused by invalid LDAP requests were found in Hitachi Directory Server Version 2:

- Invalid LDAP requests cause memory leaks and DoS.
- Invalid LDAP requests cause buffer overflow.

Malicious remote users can exploit the buffer overflow vulnerability, cause DoS of the LDAP server and execute arbitrary codes.
The fixed versions available for existing versions are indicated below. Upgrade the Hitachi Directory Server version in your system to the appropriate version.

[Affected models, versions, and fixed versions]

Product name	Model	Version	Platform	Fixed version	Release time	Last update
Hitachi Directory Server Version 2	P-2444-A124	02-11 to 02-11-/J	Windows	02-11-/K	November 28, 2006	December 21, 2006
		02-10 to 02-10-/D		02-11-/K (*1)	November 28, 2006	December 21, 2006
		02-01		02-11-/K (*1)	November 28, 2006	December 21, 2006
		02-00		02-11-/K (*1)	November 28, 2006	December 21, 2006
	P-1B44-A121	02-10 to 02-10-/U	HP-UX	02-10-/V	November 28, 2006	December 21, 2006
		02-01		02-10-/V (*1)	November 28, 2006	December 21, 2006
		02-00		02-10-/V (*1)	November 28, 2006	December 21, 2006

(*1) Please upgrade the version to a fixed revision.

For details on the fixed versions, contact your Hitachi support service representative.

[Workarounds]
Until the fixed modules are applied, please carry out the following workaround:

- Set filtering rules on the OS or router so that only reliable IP addresses can access the ports that Hitachi Directory Server Version 2 uses.

Revision history

- December 21, 2006: Information about multiple vulnerabilities of the LDAP server is released.

Page Top