

Security Vulnerability in Apache HTTP Server Affects Oracle9iAS & Oracle Http Server (OHS)

Description

A potential security vulnerability exists in Apache HTTP Servers up to and including version 1.3.24. A knowledgeable and malicious user can exploit this vulnerability by remotely sending a carefully crafted invalid request to the Apache HTTP server using chunked encoding. Doing so may lead to successful Denial of Service (DoS) attacks on 32-bit Unix operating systems and running of arbitrary code on Windows and 64-bit Unix operating systems.

This potential security vulnerability is described in detail in the Apache Security Advisory dated June 17, 2002 and available at <http://httpd.apache.org>. Additional information can be found at <http://cve.mitre.org/> under `CAN-2002-0392'.

Products affected

- OHS 1.0.2.1s for Apps only
- OHS 1.0.2.2 based on #2120450
- OHS 1.0.2.2 Roll up 2
- OHS 9.0.2
- OHS for Server 8.1.7
- OHS for Server 9.0.1
- OHS for Server 9.2

Platforms affected

- Solaris
- Windows NT
- HP
- Linux
- AIX
- Tru64

Workarounds

None

Patch Information

Oracle has fixed this potential security vulnerability under base bug number 2424256. Product Development is currently working on the fix for this issue. Patches for Windows NT and Sun Solaris will become available June 24th and June 25th. Patches for all other affected platforms will become available throughout the week of June 24th, with an expected completion by July 3rd.

Immediate patches for the base bug fix number 2424256 are being made available only for supported releases of Oracle9iAS: these are Release 2 (9.0.2), Release 1.0.2.2 and Release 1.0.2.1s (for Oracle Applications).

Patches under the same base bug number (2424256) are being made available for Oracle HTTP Server Release 9.0.1 (for Oracle9i Database) and Oracle HTTP Server Release 9.2.0 (for Oracle9iR2 Database) on all supported platforms.

When released by Oracle, Oracle9iAS Release 2 (9.0.2) for Windows and future releases of Oracle9iAS will include the fix to the potential security vulnerability described above by default.

Download currently available patches for your platform from Oracle Support Services web site, MetaLink, <http://metalink.oracle.com/>. Activate the "Patches" button to get the patches Web page. Enter bug 2424256 and activate the "Submit" button.

Please check with MetaLink or Oracle Support Services periodically for patch availability if the patch for your platform is not available.

Oracle strongly recommends that you comprehensively test the stability of your system upon application of any patch prior to deleting any of the original file(s) that are replaced by the patch.

Patch Availability Matrix

Version	Download Release	Solaris	NT	HP	Linux	AIX	Tru64
OHS 1.0.2.1s for Apps only*	OHS 1.3.12	6/24/02	6/24/02	6/26/02	TBD	6/26/02	6/26/02
OHS 1.0.2.2 based on #2120450	OHS 1.3.19	6/24/02	6/24/02	6/26/02	6/26/02	6/26/02	6/26/02
OHS 1.0.2.2**+	iAS 1.0.2	6/25/02	6/24/02	TBD	TBD	TBD	TBD
OHS 9.0.2+	iAS 9.0.2	6/24/02	InRelease	TBD	TBD	InRelease	InRelease
OHS for Server 8.1.7 ***	Oracle 8.1.7.0	6/26/02	6/26/02	TBD	TBD	TBD	TBD
OHS for Server 9.0.1	Oracle 9.0.1.0	6/26/02	6/25/02	TBD	6/26/02	6/26/02	6/26/02

OHS for Server 9.2	Oracle 9.2.0	6/26/02	6/26/02	6/26/02	6/26/02	6/26/02	6/26/02
--------------------	--------------	---------	---------	---------	---------	---------	---------

* OHS 1.0.2.1s was built for Apps 11i customers for upgrade to 1.0.2.1. It is a required upgrade for this patch.

** This includes OHS 1.0.2.2 with all of the Rollup patches that have been released for 1.0.2.2. It is a superset of OHS 1.0.2.2 based on #2120450. This Rollup 2 is currently only available on NT and Solaris.

*** Release status for OHS for Server 8.1.7 will be determined by Wednesday 7/3/02.

+ You must be on at least 9iAS 1.0.2.2. Start the Oracle Installer to determine your 9iAS version.

Credits

Oracle Corporation thanks Mark Litchfield of Next Generation Security Software Limited for discovering and bringing this potential security vulnerability to Oracle's attention.

Change Record

This alert was modified 1-July-2002 by adding the **Patch Availability matrix** and the products, platforms affected and the availability of patches was clarified.