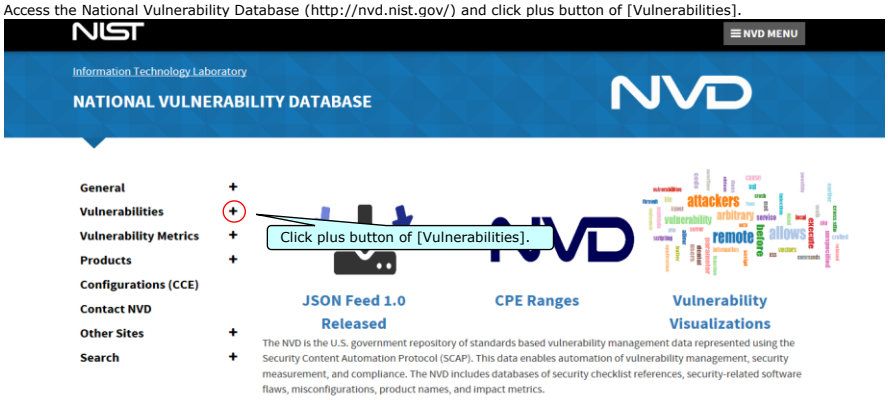
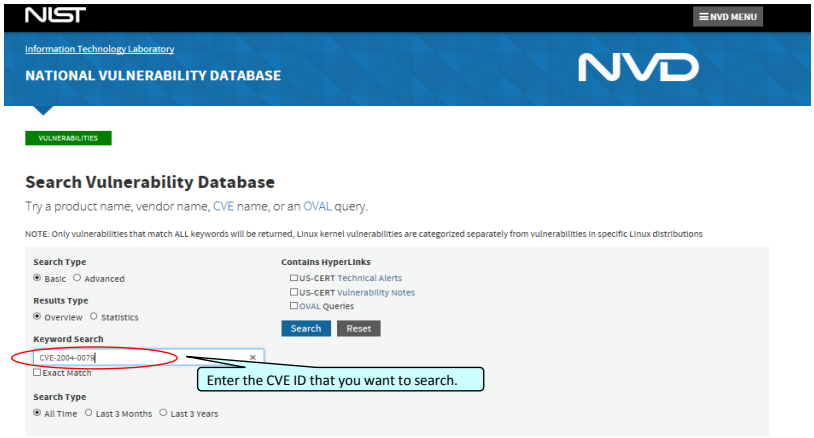
This instruction is described in "Public Server Vulnerability CountermeasuresOperation Manual", which is provided at "INSITE."
INSITE FF GROUP > System / Network > Documents Relating to the Operation of Publicly Accessible Servers
If you can't access to INSITE, please contact us at ff-websecurity@fujifilm.com.

1) Access the National Vulnerability Database (http://nvd.nist.gov/) and click plus button of [Vulnerabilities].

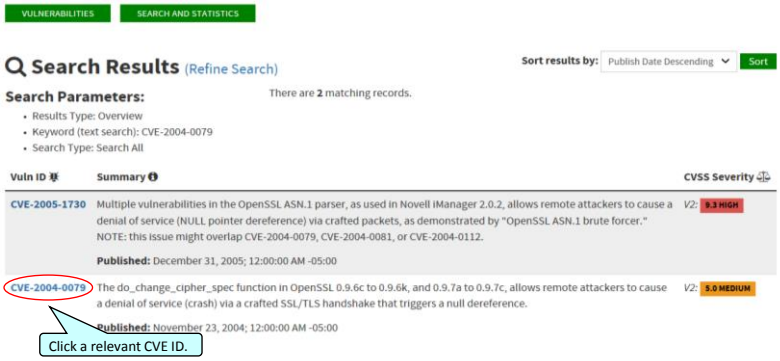


2) Click [Search & Statistics].

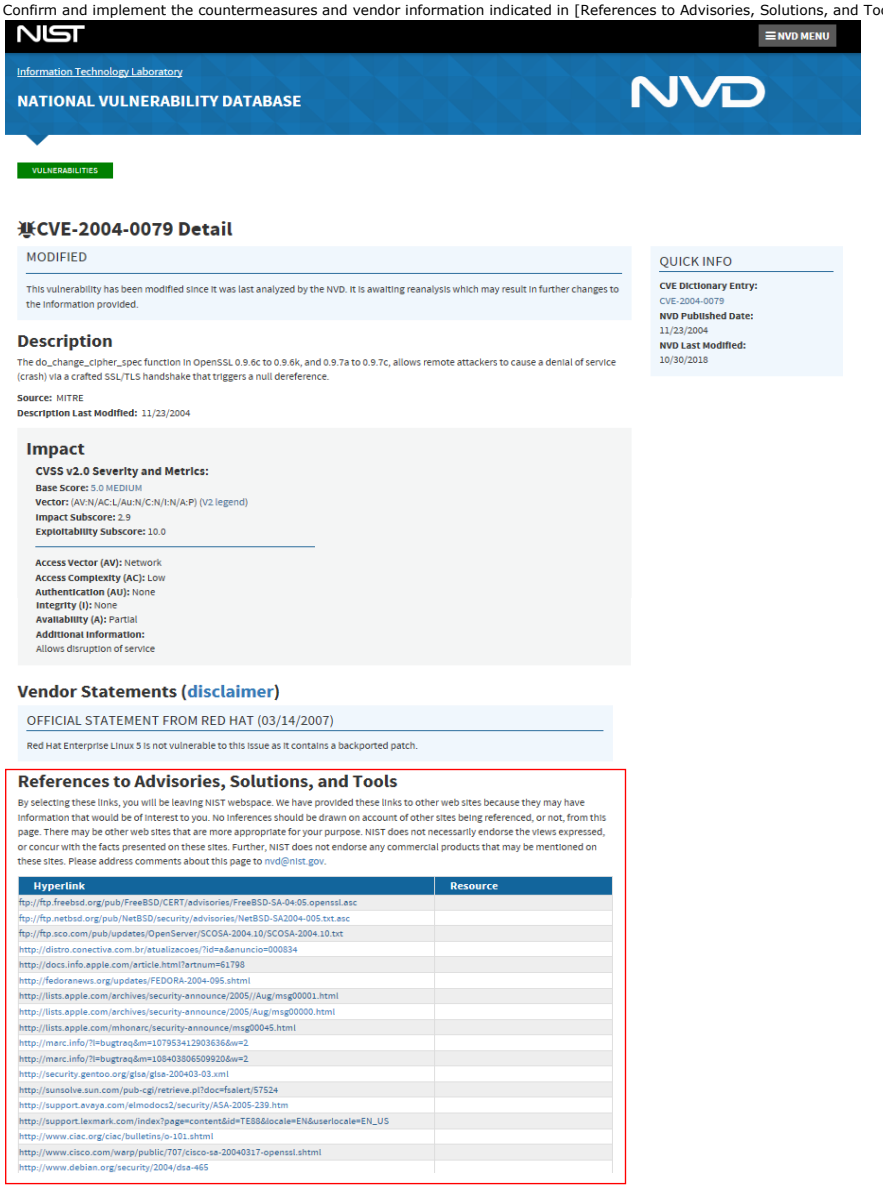
3) Enter the CVE ID that you want to search in [Keyword Search] and click [Search].



4) Click a relevant CVE ID from [Search Results].



5) Confirm and implement the countermeasures and vendor information indicated in [References to Advisories, Solutions, and Tools].



NIST NVD MENU

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NVD

VULNERABILITIES

CVE-2004-0079 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

The do_change_cipher_spec function in OpenSSL 0.9.6c to 0.9.6k, and 0.9.7a to 0.9.7c, allows remote attackers to cause a denial of service (crash) via a crafted SSL/TLS handshake that triggers a null dereference.

Source: MITRE
Description Last Modified: 11/23/2004

QUICK INFO

CVE Dictionary Entry:
CVE-2004-0079
NVD Published Date:
11/23/2004
NVD Last Modified:
10/30/2018

Impact

CVSS v2.0 Severity and Metrics:
Base Score: 5.0 MEDIUM
Vector: (AV:N/AC:L/Au:N/C:N/I:N/A:P) (V2 legend)
Impact Subscore: 2.9
Exploitability Subscore: 10.0

Access Vector (AV): Network
Access Complexity (AC): Low
Authentication (AU): None
Integrity (I): None
Availability (A): Partial
Additional Information:
Allows disruption of service

Vendor Statements (disclaimer)

OFFICIAL STATEMENT FROM RED HAT (03/14/2007)

Red Hat Enterprise Linux 5 is not vulnerable to this issue as it contains a backported patch.

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-04:05.openssl.asc	
ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-005.txt.asc	
ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2004.10/SCOSA-2004.10.txt	
http://distro.conectiva.com.br/atualizacoes/?id=a&anuncio=000834	
http://docs.info.apple.com/article.html?artnum=61798	
http://fedoranews.org/updates/FEDORA-2004-095.shtml	
http://lists.apple.com/archives/security-announce/2005//Aug/msg00001.html	
http://lists.apple.com/archives/security-announce/2005/Aug/msg00000.html	
http://lists.apple.com/mhonarc/security-announce/msg00045.html	
http://marc.info/?l=bugtraq&m=107953412903636&w=2	
http://marc.info/?l=bugtraq&m=108403806509920&w=2	
http://security.gentoo.org/glsa/glsa-200403-03.xml	
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57524	
http://support.avaya.com/elmodocs2/security/ASA-2005-239.htm	
http://support.lexmark.com/index?page=content&id=TE88&locale=EN&userlocale=EN_US	
http://www.ciac.org/ciac/bulletins/o-101.shtml	
http://www.cisco.com/warp/public/707/cisco-sa-20040317-openssl.shtml	
http://www.debian.org/security/2004/dsa-465	

* If you are unable to find the appropriate countermeasure by follwing above,
check the Results Details field on NESSUS HTML Report that we have provided.

* Any changes on the server to be made must be tested on a test environment first.

If you have any questions, please feel free to contact us at ff-websecurity@fujifilm.com.