

## **ATTENTION**

**THIS IS A DOD COMPUTER SYSTEM. BEFORE PROCESSING CLASSIFIED INFORMATION, CHECK THE SECURITY ACCREDITATION LEVEL OF THIS SYSTEM. DO NOT PROCESS, STORE, OR TRANSMIT INFORMATION CLASSIFIED ABOVE THE ACCREDITATION LEVEL OF THIS SYSTEM. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS AND NETWORK DEVICES (INCLUDES INTERNET ACCESS) ARE PROVIDED ONLY FOR AUTHORIZED U.S. GOVERNMENT USE. DOD COMPUTER SYSTEMS MAY BE MONITORED FOR ALL LAWFUL PURPOSES, INCLUDING, TO ENSURE THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY, AND OPERATIONAL SECURITY. MONITORING INCLUDES, BUT IS NOT LIMITED TO, ACTIVE ATTACKS BY AUTHORIZED DOD ENTITIES TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM. DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM MAY BE MONITORED. USE OF THIS DOD COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORING. UNAUTHORIZED USE OF THIS DOD COMPUTER SYSTEM MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR ALL LAWFUL PURPOSES.**

# CONUS TNOSC - RCERT

**FOR OFFICIAL USE ONLY**  
**CONUS THEATER NETWORK OPERATIONS AND SECURITY CENTER**  
**CONUS TNOSC TASK ORDER**  
**CT-2003-TO-0028**  
**SEPTEMBER 26, 2003**  
**FORT HUACHUCA, ARIZONA**

**SUBJECT:** Submit Web Server/Web Proxy List

**SUMMARY:** In anticipation of a task order to block inbound ports 80 and 443 on Army Security Routers and other Army routers with direct connections to WANs other than NIPRNET, this Task Order calls for identification of reverse web proxy servers, web sites not serviced by reverse proxy servers, and critical systems which require ports 80 or 443. To expedite the processing of critical Army web services, we are asking that your first submission include only your 10 most critical non-proxied web sites/reverse web proxies you manage or other servers that require port 80 or 443. Please indicate these as Level 1 (Mission Critical). RCERT managed reverse web proxies are already being submitted by the C-TNOSC/RCERT-C. A Data Entry Form has been developed and placed on the NETCROP for this data call (See Data Entry Form below). A second submission is due two days afterward for remaining devices using ports 80 or 443. You should prioritize these later entries by indicating Level 2 (Informational) or Level 3 (Not Critical) in the data entry form.

**REFERENCES:**

1<sup>st</sup> I/O Command Tasking Order TO2003-0071 181730Z Sep 2003  
Army IAVA A2003-0023 Buffer Overrun In RPCSS, 09/11/2003  
DOD CERT IAVA 2003-A-0012  
<ftp://www.cert.mil/pub/bulletins/dodcert2003/2003-a-0012.htm>  
CERT/CC Advisory CA-2003-23  
<http://www.cert.org/advisories/CA-2003-23.html>  
Microsoft Security Bulletin MS03-039  
[http://www.microsoft.com/security/security\\_bulletins/ms03-039.asp](http://www.microsoft.com/security/security_bulletins/ms03-039.asp)  
C-TNOSC Warning Order CT-2003-WO-0012

**SUSPENSE:** 301900Z SEP 03 Level 1 Devices and Reverse Web Proxies  
021900Z OCT 03 Remaining Non-Proxied Web Sites

**Classification:** UNCLASSIFIED (FOUO)

**SITUATION:** An exploit against the vulnerability identified in the references is publicly available and it is anticipated that the release of a network worm using this exploit is a serious possibility within a matter of days. A worm would rapidly propagate and infect vulnerable hosts throughout the Army portion of the GIG. The ANSOC/ACERT would like to apply a block to all port 80 and 443 **into, not within,** Army

installations. ***These blocks will affect traffic between Army installations.*** These blocks will need to have many exceptions, or they will have a significant impact to our Army missions. This data call is to identify those exceptions. Exceptions must be evaluated (scanned) by RCERT-C for vulnerabilities and considered for placement behind reverse proxy servers. While placement behind reverse proxy servers is preferable, it is understood that some servers cannot operate in this configuration. RCERT approved reverse proxy servers and servers evaluated by RCERT and determined unsuitable for reverse proxy will be considered for exceptions. C-TNOSC will notify our customers as early as we can should the ANSOC/ACERT direct a block. At this time, DISA has made no plans to block these ports unless absolutely necessary to protect the operation of the DISN. Exceptions approved through this data call will be pre-positioned on Army Security Routers and will be submitted to DISA so that pre-positioned exceptions can be developed for use on DISA Internet Access Points( IAP).

### **TASK AND PURPOSE:**

**Task:** Using the Data Entry Form on NETCROP (see below), submit data on reverse web proxies, non-proxied web sites, or other critical devices that will be affected by a block to ports 80 and 443. For those that have already responded to Warning Order CT-2003-WO-0012A or Task Order CT-2003-TO-0027, and have submitted device information, it is not necessary to re-submit the data. However, a member from the ARM Team will contact you for any additional information now required.

1. Using the Data Entry Form on NETCROP (see below), submit Level 1 (up to 10 of your most critical) devices that would be impacted by a block on ports 80 and 443. The suspense date for this submission is 301900Z SEP 03. Submissions after the suspense date will not be considered as Level 1.
2. Using the Data Entry Form on NETCROP (see below), submit a list of Level 2 and 3 devices that would be impacted by a block on ports 80 and 443. The suspense date for this submission is 021900Z OCT 03.

**Purpose:** The purpose is to gather data of critical devices that would be impacted by a block of ports 80 and 443. The highest priority devices (Level 1) will be submitted first. These will be evaluated by RCERT-C for vulnerabilities and considered for placement behind reverse proxy servers. Next, lower priority devices (Level 2 and 3) will be submitted and evaluated by RCERT-C and considered for placement behind reverse proxy servers. After the submission and evaluation of these devices (unless circumstances require more immediate actions) ANOSC will consider directing the blocking of all port 80 and 443 on Army Security Routers and Army interfaces to external WANs, such as DREN and ISPs. ANOSC will submit verified exceptions (submitted and evaluated) to DISA so that if DISA is directed to block port 80 and 443 traffic some time in the future, Army exceptions will already have been submitted.

### **ACTIONS REQUIRED:**

1. FCIOs: NGB, Reserves, COE, MEDCOM, and CFSC report acknowledgement by 291900Z SEP 03 to NEAR CT-2003-TO-0028 on all of your entries in the DOIM section and FCIO section. Submit exception candidates using the Data Entry Form on NETCROP (see below). Note Level 1 suspense date and Level 2 & 3 suspense date above. Report compliance on NEAR after all information has been submitted.

2. RCIOs: Northeast, Northwest, Southeast, Southwest report acknowledgement by 291900Z SEP 03 to NEAR CT-2003-TO-0028. All sites in your region must report acknowledgement to NEAR CT-2003-TO-0028 and will submit exception candidates using the Data Entry Form on NETCROP (see below). Note Level 1 suspense date and Level 2 & 3 suspense date above. Sites in your region must report compliance on NEAR after all information has been submitted for Level 1, 2, and 3 devices; RCIOs will report compliance for the region.
3. DOIM and DOIM-like activities: Report acknowledgement by 291900Z SEP 03 to NEAR CT-2003-TO-0028. Submit exception candidates using the Data Entry Form on NETCROP (see below). Note Level 1 suspense date and Level 2 & 3 suspense date above. Report compliance on NEAR after all information has been submitted for Level 1, 2, and 3 devices.
4. Commands, Special Reporting Activities, PEOs report acknowledgement by 291900Z SEP 03 to NEAR CT-2003-TO-0028. Submit exception candidates using the Data Entry Form on NETCROP (see below). Note Level 1 suspense date and Level 2 & 3 suspense date above. Report compliance on NEAR to the Command/Special Reporting Activity/PEO sections of the NETCROP NEAR after all information has been submitted for Level 1, 2, and 3 devices.

**DATA ENTRY FORM:**

Log in to NETCROP

On the left hand side, scroll down to Data Call

Select Web Server Registration

**Please note that with this form, you can only see registrations that “you” entered under your UserId; there is no ability to view registrations that someone else entered. There is also no ability to edit existing registrations. Due to time constraints it is basically a simple data entry form.**

CONUS-TNOSC Action Request Management Team  
NETC-ANC-N  
Fort Huachuca, AZ 85613  
conus-tnosc-arm@netcom.army.mil  
Comm. (520) 533-1854, DSN 821-1854