JTF-CNO COMMANDERS NETWORK VULNERABILITY ALERT 02-01

From: *owner-csa@infosec.navy.mil*
Date: 03/01/02

- **Previous message:** owner-csa@infosec.navy.mil: "NAVY-WIDE ISSM SYMPOSIUM"

ROUTINE
R 010002Z MAR 02 PSN 925089J33
FM NCTF-CND WASHINGTON DC
TO UNSECNAV WASHINGTON DC//AAUSN// CINCLANTFLT NORFOLK VA CNET PENSACOLA FL BUMED WASHINGTON DC CNR ARLINGTON VA COMNAVAIRSYSCOM PATUXENT RIVER MD COMNAVDIST WASHINGTON DC COMNAVFACENGCOM WASHINGTON DC COMNAVLEGSVCCOM WASHINGTON DC COMNAVMETOCCOM STENNIS SPACE CENTER MS COMNAVNETOPSCOM WASHINGTON DC COMNAVPERSCOM MILLINGTON TN COMNAVRESFOR NEW ORLEANS LA COMNAVSAFECEN NORFOLK VA COMNAVSEASYSCOM WASHINGTON DC COMNAVSECGRU FT GEORGE G MEADE MD COMNAVSUPSYSCOM MECHANICSBURG PA COMOPTEVFOR NORFOLK VA COMSC WASHINGTON DC DIRSSP WASHINGTON DC FLDSUPPACT WASHINGTON DC NAVHISTCEN WASHINGTON DC NAVOBSY WASHINGTON DC NAVWARCOL NEWPORT RI OGC WASHINGTON DC ONI WASHINGTON DC PRESINSURV NORFOLK VA USNA ANNAPOLIS MD ZEN/CINCPACFLT PEARL HARBOR HI ZEN/CINCUSNAVEUR LONDON UK ZEN/CINCUSNAVEUR LONDON UK ZEN/COMNAVSPACECOM DAHLGREN VA ZEN/COMNAVSPACECOM DAHLGREN VA ZEN/COMNAVSPECWARCOM CORONADO CA ZEN/COMNAVSPECWARCOM CORONADO CA ZEN/TIONS/L=VIRGINIA/L=NORFOLK/OU=COMOPTEVFOR NORFOLK VA(N) ZEN/COMSPAWARSYSCOM SAN DIEGO CA ZEN/COMSPAWARSYSCOM SAN DIEGO CA ZEN/COMUSNAVCENT ZEN/NAVPGSCOL MONTEREY CA ZEN/NAVPGSCOL MONTEREY CA ZEN/NAVSTKAIRWARCEN FALLON NV ZEN/NAVSTKAIRWARCEN FALLON NV ZEN/NCTSI SAN DIEGO CA ZEN/NCTSI SAN DIEGO CA ZEN/UNSECNAV WASHINGTON DC
INFO ALCND CNO WASHINGTON DC RUEHMD/USDAO MADRID SP RUEHBR/USDAO BRASILIA BR COMDT COGARD WASHINGTON DC RUEHJI/NAVFORDIVMTM DET JEDDAH SA DISA WASHINGTON DC JTF-CNO WASHINGTON DC FLTINFOWARCEN NORFOLK VA ZEN/NCTF-CND WASHINGTON DC

THIS IS A 2 SECTIONED MSG COLLATED BY MDS UNCLAS FOUO

SUBJ: JTF-CNO COMMANDERS NETWORK VULNERABILITY ALERT 02-01 ALCND 013/02
MSGID/GENADMIN/NCTF-CND/-/FEB//

SUBJ/JTF-CNO COMMANDERS NETWORK VULNERABILITY ALERT 02-01//
REF/A/GENADMIN/JTF-CNO/280321ZFEB02/-/NOTAL//
REF/B/GENADMIN/NCTF-CND/271919ZAUG01//
REF/C/GENADMIN/NCTF-CND/212017ZSEP01//
REF/D/DOC/CNO/30NOV2001//
REF/E/GENADMIN/NCTF-CND/042053ZJAN02//
NARR/REF A IS JTF-CNO COMMANDERS NETWORK VULNERABILITY ALERT 02-01, NULL/DEFAULT PASSWORDS AND UNPATCHED SOFTWARE/SYSTEMS. REF B IS IAVA 2001-A-5001, CODE RED WORM PATCH RE- VERIFICATION, SEE LINKS FROM https://INFOSEC.NAVY.MIL/ADVISORY (LOWER CASE). REF C IS IAVA 2001-A-0010.0.0 MULTIPLE VULNERABILITIES IN MICROSOFT IIS , SEE LINKS FROM https://INFOSEC.NAVY.MIL/ADVISORY (LOWER CASE). REF D IS NAVY-MARINE CORPS NIPRNET ENCLAVE PROTECTION POLICY, SEE LINKS FROM https://INFOSEC.NAVY.MIL/FLEET (LOWER CASE). REF E IS ALCND 002/02, NIPRNET ENCLAVE PROTECTION POLICY ON FILE TRANSFER PROTOCOL, SEE http://WWW.NCTC.NAVY.SMIL.MIL/NCTF/ CND00202.HTML (LOWER CASE/SIPRNET).// POC/F.Q. MEZA/LCDR/NCTF-CND/LOC:WASHINGTON DC/TEL:COMM (202)764- 0755 DSN: 764-0755/EMAIL: MEZAF@NCTC.NAVY.MIL//
RMKS/1. BACKGROUND. REF A, WHICH IS QUOTED BELOW FOR YOUR INFORMATION, DETAILS CONCERNS BY JTF-CNO OF THE RISE IN THE NUMBER OF INTRUSIONS INTO DOD NETWORKS ATTRIBUTED TO UTILIZING DEFAULT PASSWORDS, UNPATCHED SOFTWARE/SYSTEMS, AND IMPROPER USE OF REMOTE ACCESS APPLICATIONS.
2. IN ADDITION TO NETWORK SECURITY CONCERNS EXPRESSED IN REF A, NCTF-CND HAS ALSO NOTED A NUMBER OF COMPUTER NETWORK INCIDENTS THAT CONTINUE TO EXPLOIT VULNERABILITIES IN DIFFERENT IMPLEMENTATIONS OF FILE TRANSFER PROTOCOL (FTP), OR THAT USE FTP TO EXPLOIT HOSTS WITH IMPROPERLY SECURED SYSTEMS. IN THE VAST MAJORITY OF CASES, THE PROBLEM WAS ONE OR MORE OF THE FOLLOWING:
A. FTP SERVICES WERE INSTALLED ON A HOST BY DEFAULT AND WERE RUNNING WITHOUT KNOWLEDGE OF THE SYSADMIN.
B. FTP WAS USED TO DEGRADE OR DESTROY A FILE SYSTEM THAT WAS SET UP WITH EXCESSIVE PERMISSIONS.
C. UNPATCHED FTP SOFTWARE ALLOWED AN INTRUDER TO GET ROOT ACCESS ON THE HOST.
3. ADDITIONALLY, NAVY SYSTEMS RUNNING MICROSOFT'S INTERNET INFORMATION SERVER (IIS) CONTINUE TO BE EXPLOITED BY THE CODE RED WORM OR THE NIMDA WORM DESPITE DIRECTED INSTALLATION OF THE CURRENT IIS SECURITY PATCH IN IAVA 2001-A-5001 (REF B) AND IAVA 2001-A-0010 (REF C). FACTORS THAT HAVE CONTRIBUTED TO CONTINUED EXPLOITATION OF IIS INCLUDE THE FOLLOWING:
A. SYSADMIN WAS UNAWARE OF THE EXISTENCE OF A SERVER UNTIL IT BECAME INFECTED.
B. SYSADMIN DID NOT PATCH A SERVER UNDER THE CONTROL OF A TENANT COMMAND OR A CONTRACTOR, SINCE THERE WAS NO FORMAL MEMORANDUM OF AGREEMENT THAT SPECIFIED WHO IS RESPONSIBLE FOR PATCHING SUCH HOSTS.
C. SECURITY PATCH WAS NOT PROPERLY INSTALLED.
D. SECURITY PATCH INSTALLED, BUT SYSADMIN FAILED TO REBOOT THE HOST AND THE PATCH DID NOT PROPERLY INSTALL.
E. SECURITY PATCH INSTALLED, BUT SYSADMIN REBUILT A SYSTEM FOLLOWING SYSTEM CRASH OR FAILURE AND DID NOT REINSTALL THE PATCH.
4. IN EFFORT TO REDUCE THE NUMBER OF COMPUTER NETWORK INCIDENTS,

RECOMMEND TAKING THE FOLLOWING STEPS TO FURTHER ENHANCE THE SECURITY OF ALL NAVY NETWORKS:
A. ENSURE SYSTEMS ARE IN COMPLIANCE WITH REF D, NAVY AND MARINE CORPS NIPRNET ENCLAVE PROTECTION POLICY.
B. ENSURE SYSTEMS ARE NOT VULNERABLE TO FTP EXPLOITATIONS AS NOTED IN PARA 2 ABOVE (REF E GERMANE).
C. ENSURE SYSTEMS ARE NOT VULNERABLE TO IIS EXPLOITATION AS NOTED IN PARA 3 ABOVE (REF B & C GERMANE).
D. ENSURE THAT SYSADMIN ACCOUNTS OR ANY OTHER ACCOUNTS DO NOT HAVE NULL/DEFAULT PASSWORDS SET.
5. ALTHOUGH THIS MESSAGE WILL NOT BE TRACKED VIA OCRS NOR IS THERE A REQUIREMENT TO REPORT COMPLIANCE, NCTF-CND REQUESTS THAT ALL COMMANDERS LEND THEIR FULL ATTENTION IN ENSURING NETWORK SECURITY VULNERABILITIES MENTIONED ABOVE AND IN REF A ARE ADDRESSED AT EVERY LEVEL.
6. THE JTF-CNO MESSAGE,REF A, IS QUOTED BELOW TO ENSURE WIDEST DISSEMINATION: QUOTE R 280321Z FEB 02 FM JTF CNO WASHINGTON DC//J3//
SUBJ: COMMANDERS NETWORK VULNERABILITY ALERT 02-01, NULL/DEFAULT PASSWORDS AND UNPATCHED SOFTWARE/SYSTEMS 1. (U) JTF-CNO HAS DOCUMENTED A RISE IN THE NUMBER OF INTRUSIONS INTO DOD NETWORKS ATTRIBUTED TO UTILIZING DEFAULT PASSWORDS, UNPATCHED SOFTWARE/SYSTEMS, AND IMPROPER USE OF REMOTE ACCESS APPLICATIONS. IN SOME CASES, THESE INTRUSIONS HAVE APPARENTLY STOPPED AT THE COMPROMISED MACHINE. IN OTHERS, THE INTRUDER IS ABLE TO HOP TO OTHER NETWORKED MACHINES OR OTHER ENTIRE NETWORKS. THESE INTRUSION SETS ARE COSTLY AND TIME CONSUMING TO UNRAVEL, AND ILLUSTRATE THE ABSOLUTE NECESSITY TO PROPERLY EMPLOY STRICT SECURITY MEASURES. 2. (U) DURING THE LAST FEW MONTHS, DOD LAW ENFORCEMENT REPORTED ON AN INTRUSION SET INVOLVING COMPROMISED UNCLASSIFIED DOD MACHINES THAT DATES BACK TO FALL 2001. THE INITIAL INTRUSION APPEARED TO ORIGINATE FROM OUTSIDE CONUS. BY USING DEFAULT PASSWORDS, THE INTRUDER(S) SUCCESSFULLY GAINED ROOT ACCESS TO SEVERAL MACHINES ON A HOST OF DIFFERENT NETWORKS. IN SEVERAL CASES THE INTRUDER(S) INSTALLED REMOTE ACCESS TOOLS, AND IN THE MOST RECENTLY DETECTED CASE, HE DELETED USER ACCOUNTS AND CRITICAL SYSTEM FILES. THERE ARE MANY AVAILABLE REMOTE ACCESS TOOLS WIDELY AVAILABLE ON THE INTERNET THAT WILL ALLOW AN INTRUDER CONTINUED ACCESS TO A COMPROMISED MACHINE. IN ALL, OVER 15 MACHINES WERE COMPROMISED AT THE ROOT LEVEL BY THIS INTRUDER(S). THE OVERALL COST IN DOLLARS, LOST PRODUCTIVITY, AND INFORMATION IS YET TO BE DETERMINED. THIS INTRUSION SET IS STILL BEING PURSUED BY LAW ENFORCEMENT, AND THE DETAILS ARE CONSIDERED LAW ENFORCEMENT SENSITIVE. AT THE CONCLUSION OF THE INVESTIGATION JTF-CNO WILL RELEASE A MORE DETAILED ACCOUNT OF THE INTRUDERS ACTIVITY. 3. (U) COMMANDERS MUST ENSURE THAT INFORMED DECISIONS ARE BEING MADE REGARDING THE INSTALLATION, OPERATION, AND CONFIGURATION OF ALL OPERATING SYSTEMS AND APPLICATIONS INCLUDING REMOTE ACCESS APPLICATIONS SUCH AS "REMOTELY ANYWHERE", "PC ANYWHERE", AND OTHER COMMONLY AVAILABLE REMOTE ACCESS SOFTWARE. SYSTEM ADMINISTRATORS MUST ENSURE ALL SYSTEMS HAVE STRONG PASSWORDS FOR LOCAL ADMINISTRATOR ACCOUNTS AND SHOULD ENFORCE THE USE OF STRONG USER PASSWORDS THROUGH PASSWORD POLICY ENFORCEMENT. ADDITIONALLY, ALL SYSTEM ADMINISTRATOR SOFTWARE

MUST BE SURVEYED AND ENSURED TO BE STRICTLY LOCKED DOWN, ALLOWING ACCESS ONLY TO THOSE WITH ADMINISTRATIVE PRIVILEGES. 4. (U) JTF-CNO NEEDS THE FULL ATTENTION AND SUPPORT OF ALL OPERATIONAL COMMANDERS IN ADDRESSING THIS GRAVE VULNERABILITY TO OUR NETWORKS AND OUR INFORMATION. THE THREAT IS REAL, AND THE POTENTIAL IMPACT TO OUR OPERATIONS IS PROFOUND. THE TASK OF REMAINING TECHNICALLY AHEAD OF THE THREAT IS DIFFICULT ENOUGH; WE MUST DO BETTER AT SECURING OUR NETWORKS FROM THOSE THAT ARE SIMPLY LOOKING TO EXPLOIT OVERSIGHTS IN OUR DEFENSIVE POSTURE. 5. (U)POINT OF CONTACT: JOINT TASK FORCE WATCH OFFICER

DSN: (312) 327-4583, COMM (703) 607-4583
NIPR: JTFWO@JTFCNO.IA.MIL
SIPR: JTFWO@JTFCNO.IA.SMIL.MIL UNQUOTE//
BT NNNN

SSL-enabled Version https://infosec.navy.mil/ PKI-enabled Version https://warlord.spawar.navy.mil/
(Requires a DoD Certificate) SIPRNET Version infosec.navy.smil.mil Bulletin Board Version (NEBBS) DSN: 588.4873/3496 COMM: 843.218.4873/3496

NAVY ITAC - Toll Free: 800.304.4636 DSN: 588.5426/4286 COM: 843.218.5426/4286 E-mail: itac@infosec.navy.mil

---

- **Previous message:** owner-csa@infosec.navy.mil: "NAVY-WIDE ISSM SYMPOSIUM"

About this list	Date view	Thread view	Subject view	Author view

SPAWAR

Administration provided by the
SPAWAR Systems Center
in Charleston, South Carolina, USA.
itac@infosec.navy.mil