x0rz / **EQGRP**

Watch 387 | Star 3,397 | Fork 2,083

Code | Issues 13 | Pull requests 1 | Projects 0 | Insights

Decrypted content of eqgrp-auction-file.tar.xz

exploits shadowbrokers equationgroup hacking nsa tao

33 commits | 1 branch | 0 releases | 5 contributors

Branch: **master** ▾ New pull request Find file Clone or download ▾

x0rz Merge pull request #28 from inso-/patch-10 … Latest commit `0c2354f` on Apr 12, 2017

Linux	add untracked files	a year ago

archive_files	Added all the files inside compressed bz2 and gz files	a year ago
README.md	Update ITIME	a year ago

README.md

Browsable content of eqgrp-auction-file.tar.xz

- Original file: https://mega.nz/#!zEAU1AQL!oWJ63n-D6lCuCQ4AY0Cv_405hX8kn7MEsa1iLH5UjKU
- Passphrase: `CrDj"(;Va.*NdlnzB9M?@K2)#>deB7mN` (as disclosed by the ShadowBrokers, source)
- This summary is provided by the community: complaints/credits to `jvoisin` @ `dustri.org` and @x0rz

⚠️ Some binaries may be picked up by your antivirus

Nested Tar archives have been uncompressed in the archive_files folder.

Content

Unknown

- **JACKLADDER**
- **DAMPCROWD**
- **ELDESTMYDLE**
- **SUAVEEYEFUL**

- **WATCHER**
- **YELLOWSPIRIT**

Misc

- **DITTLELIGHT (HIDELIGHT)** unhide **NOPEN** window to run unix oracle db scripts
- **DUL** shellcode packer
- **egg_timer** execution delayer (equivalent to `at`)
- **ewok** snmpwalk-like?
- **gr** Web crontab manager? wtf. NSA are webscale dude
- **jackladderhelper** simple port binder
- **magicjack** DES implementation in Perl
- **PORKSERVER** inetd-based server for the **PORK** implant
- **ri** equivalent to `rpcinfo`
- **uX_local** Micro X server, likely for remote management
- **ITIME** Change Date/Time of a last change on a file of an unix filesystem

Remote Code Execution

Solaris

- **CATFLAP** Solaris 7/8/9 (SPARC and Intel) RCE (for a **LOT** of versions)
- **EASYSTREET**/**CMSEX** and **cmsd** Solaris `rpc.cmsd` remote root

- **EBBISLAND/ELVISCICADA/snmpXdmid** and **frown**: `CVE-2001-0236`, Solaris 2.6-2.9 - snmpXdmid Buffer Overflow
- **sneer**: *mibissa* (Sun snmpd) RCE, with *DWARF* symbols :D
- **dtspcdx_sparc** dtspcd RCE for SunOS 5. -5.8. what a useless exploit
- **TOOLTALK** DEC, IRIX, or Sol2.6 or earlier Tooltalk buffer overflow RCE
- **VIOLENTSPIRIT** RCE for ttsession daemon in CDE on Solaris 2.6-2.9 on SPARC and x86
- **EBBISLAND** RCE Solaris 2.6 -> 2.10 Inject shellcode in vulnerable rpc service

Netscape Server

- **xp_ns-httpd** NetScape Server RCE
- **nsent** RCE for NetScape Enterprise server 4.1 for Solaris
- **eggbasket** another NetScape Enterprise RCE, this time version `3.5`, likely SPARC only

FTP servers

- **EE** proftpd 1.2.8 RCE, for RHL 7.3+/Linux, `CVE-2011-4130`? another reason not to use proftpd
- **wuftpd** likely `CVE-2001-0550`

Web

- **ESMARKCONANT** exploits phpBB remote command execution (<2.0.11) `CVE-2004-1315`
- **ELIDESKEW** Public known vulnerablity in SquirrelMail versions 1.4.0 - 1.4.7
- **ELITEHAMMER** Runs against RedFlag Webmail 4, yields user `nobody`
- **ENVISIONCOLLISION** RCE for phpBB (derivative)
- **EPICHERO** RCE for Avaya Media Server

- **COTTONAXE** RCE to retrieve log and information on LiteSpeed Web Server

Misc

- **calserver** spooler RPC based RCE
- **EARLYSHOVEL** RCE RHL7 using sendmail `CVE-2003-0681` `CVE-2003-0694`
- **ECHOWRECKER/sambal**: samba 2.2 and 3.0.2a - 3.0.12-5 RCE (with *DWARF* symbols), for FreeBSD, OpenBSD 3.1, OpenBSD 3.2 (with a non-executable stack, zomg), and Linux. Likely `CVE-2003-0201`. There is also a Solaris version
- **ELECTRICSLIDE** RCE (heap-overflow) in Squid, with a chinese-looking vector
- **EMBERSNOUT** a remote exploit against Red Hat 9.0's httpd-2.0.40-21
- **ENGAGENAUGHTY/apache-ssl-linux** Apache2 mod-ssl RCE (2008), SSLv2
- **ENTERSEED** Postfix RCE, for 2.0.8 - 2.1.5
- **ERRGENTLE/xp-exim-3-remote-linux** Exim remote root, likely `CVE-2001-0690`, Exim 3.22 - 3.35
- **EXPOSITTRAG** exploit pcnfsd version 2.x
- **extinctspinash**: `Chili!Soft ASP` stuff RCE? and *Cobalt RaQ* too?
- **KWIKEMART** (**km** binary) RCE for SSH1 padding crc32 thingy (https://packetstormsecurity.com/files/24347/ssh1.crc32.txt.html)
- **prout** (ab)use of `pcnfs` RPC program (version 2 only) (1999)
- **slugger**: various printers RCE, looks like `CVE-1999-0078`
- **statdx** Redhat Linux 6.0/6.1/6.2 rpc.statd remote root exploit (IA32)
- **telex** Telnetd RCE for RHL? `CVE-1999-0192`?
- **toffeehammer** RCE for `cgiecho` part of `cgimail`, exploits fprintf
- **VS-VIOLET** Solaris 2.6 - 2.9, something related to XDMCP
- **SKIMCOUNTRY** Steal mobile phone log data
- **SLYHERETIC_CHECKS** Check if a target is ready for **SLYHERETIC** (not included)

- **EMPTYBOWL** RCE for MailCenter Gateway (mcgate) - an application that comes with Asia Info Message Center mailserver; buffer overflow allows a string passed to popen() call to be controlled by an attacker; arbitraty cmd execute known to work only for AIMC Version 2.9.5.1
- **CURSEHAPPY** Parser of CDR (Call Detail Records) (siemens, alcatel, other containing isb hki lhr files) probably upgrade of ORLEANSTRIDE
- **ORLEANSTRIDE** Parser of CDR (Call Detail Records)

Anti-forensic

- **toast**: `wtmps` editor/manipulator/querier
- **pcleans**: `pacctl` manipulator/cleaner
- **DIZZYTACHOMETER**: Alters RPM database when system file is changed so that RPM (>4.1) verify doesn't complain
- **DUBMOAT** Manipulate utmp
- **scrubhands** post-op cleanup tool?
- **Auditcleaner** cleans up `audit.log`

Control

Iting HP-UX, Linux, SunOS

- **FUNNELOUT**: database-based web-backdoor for `vbulletin`
- **hi** UNIX bind shell
- **jackpop** bind shell for SPARC

- **NOPEN** Backdoor? A RAT or post-exploitation shell consisting of a client and a server that encrypts data using RC6 source** SunOS5.8
- **SAMPLEMAN / ROUTER TOUCH** Clearly hits Cisco via some sort of redirection via a tool on port 2323... (thanks to @cynicalsecurity)
- **SECONDDATE** Implant for Linux/FreeBSD/Solaris/JunOS
- **SHENTYSDELIGHT** Linux keylogger
- **SIDETRACK** implant used for **PITCHIMPAIR**
- **SIFT** Implant for Solaris/Linux/FreeBSD
- **SLYHERETIC** SLYHERETIC is a light-weight implant for AIX 5.1:-5.2 Uses Hide-in-Plain-Sight techniques to provide stealth.
- **STRIFEWORLD**: Network-monitoring for UNIX, needs to be launched as root. Strifeworld is a program that captures data transmitted as part of TCP connections and stores the data in a memory for analysis. Strifeworld reconstructs the actual data streams and stores each session in a file for later analysis.
- **SUCTIONCHAR**: 32 or 64 bit OS, solaris sparc 8,9, Kernel level implant - transparent, sustained, or realtime interception of processes input/output vnode traffic, able to intercept ssh, telnet, rlogin, rsh, password, login, csh, su, …
- **STOICSURGEON** Rootkit/Backdoor Linux MultiArchi
- **INCISION** Rootkit/Backdoor Linux Can be upgrade to StoicSurgeon(more recent version)

CnC

- **Seconddate_CnC**: CnC for **SECONDDATE**
- **ELECTRICSIDE** likely a big-fat-ass CnC
- **NOCLIENT** Seems to be the CnC for **NOPEN***
- **DEWDROP**

Privesc

Linux

- **h**: linux kernel privesc, old-day compiled `hatorihanzo.c`, do-brk() in 2.4.22 CVE-2003-0961
- **gsh**: `setreuid(0,0);execl("bash","/bin/bash")`
- **PTRACE/FORKPTY/km3**: linux kernel lpe, kmod+ptrace, CVE-2003-0127, (https://mjt.nysv.org/scratch/ptrace_exploit/km3.c)
- **EXACTCHANGE**: NULL-deref based local-root, based on various sockets protocols, compiled in 2004, made public in 2005
- **ghost**: `statmon`/tooltalk privesc?
- **elgingamble**:
- **ESTOPFORBADE** local root `gds_inet_server` for, Cobalt Linux release 6.0, to be used with **complexpuzzle**
- **ENVOYTOMATO** LPE through bluetooth stack(?)
- **ESTOPMOONLIT** Linux LPE
- **EPOXYRESIN** Linux LPE

AIX

- **EXCEEDSALON-AIX** privesc

Others

- **procsuid**: setuid perl (yes, it's a real thing) privesc through unsanitized environnement variables. wtf dude

- **elatedmonkey**: cpanel privesc (0day) using `/usr/local/cpanel/3rdparty/mailman/`. Creates mailman mailing list: `mailman config_list`
- **estesfox**: logwatch privesc, old-day
- **evolvingstrategy**: privesc, likely for Kaspersky Anti-virus (`/sbin/keepup2date` is kaspersky's stuff) (what is `ey_vrupdate`?)
- **eh** OpenWebMail privesc
- **escrowupgrade** cachefsd for solaris 2.6 2.7 sparc
- **ENGLANDBOGY** local exploit against Xorg X11R7 1.0.1, X11R7 1.0, X11R6 6.9, Includes the following distributions: MandrakeSoft Linux 10.2, Ubuntu 5.0.4, SuSE Linux 10.0, RedHat Fedora Core5, MandrakeSoft Linux 2006.0. requires a setuid Xorg
- **endlessdonut**: Apache fastcgi privesc

Interesting stuff

- default passwords list (courtesy of x0rz)
- .gov.ru (stoicsurgeon_ctrl__v__1.5.13.5_x86-freebsd-5.3-sassyninja-mail.aprf.gov.ru) (wow!)