

CNCERT ; û à ¶ ú s

2022 v 5 Ñ È † 137 Ê



d}y

‡ q A\ » & 1 & (5 7

S K, R+ æ

Ñ) û p %o, d

- e S

³/₄ B • + ù • ô

Q "

³/₄ B • „ ³/₄

„ & *

¿ ¿ š K

³/₄ ³ ¥ ð o æ

Q d c / :

Q d

- (% ! +86108299099
(• Ñ ! cncert@cert.org
PGP Key! <http://www.cert.org>
! <http://www.cert.org>

¼ 9 ç ‹ ‘ Ñ à ì • Ä Ð Ô ò #² ¶ g

CNCERT h

1 c CNCERT Å

]’ “

³ ¥™ 8 o î ë „ • ì % 8 Ø 8 / ì Å K q³ ¥ S ë „ / ì r ç 3 Å

K CNCERT g CNCERT/CC NK 2001 - 8 e Ä ÿ Ä ô F î æ • ì

/ ì ¾ /³™ 8 o î ë „ % 8 ~ , / € È æ * d´ ³ ¥ % ë „ / ì V´

“¾! Ö q r ~ G ½ c f “ ÿ £ c Ù .¹ ë c O I K r ° ì — ° S î

æ¹ Ñ G ½ c ÿ £ c G > ä Ø 8 % ”]´ n û ä • 8³ ¥ ð o æ ° S k °

< [CNVD dk S æ I Ð ´ Í ð o n „ • æ n û d

ë „ ~ ,

´ /³™ 8 o î ë „ % 8 ~ , / € È æ * , • CNCERT } /³ Ö Ä 31

Q ~ c´ - Ö c Š Ç • Ó o r¹ ¶ ! î æ r æ c 0 Í c € V ! ä Y

N o r Ø 8 € \$ î n ì æ * c 7` û ` o r ä c P ë „ , ì r Ù /³ S

æ ë „ ~ , k ½ % ” R + S 7 Ö î æ¹ Ñ d

û æ æ´

CNCERT r ~ ÿ H û æ S N æ O 0³ • n „ (ð r æ c™ (ð r æ c 7`

_ û ` o r c î æ û ` , e Ù K ° S ð o k ° c î È] ½³ c Ý - 8 ä

Æ q k °]´ o % ! æ î æ ð o k ° ä • ì æ´ A³ æ Ó d k S î

æ û ` o r N q CNCERT î æ ë „ û ` J æ * r d CNCERT . N K t /³

± î È] S 0 ANVA ä /³ S î æ Ý - 8 S 0 CCTGA d

³ • æ´

CNCERT r ~ — ° î æ³ • æ´ ! O r Ù Ô B î æ¹ Ñ Ù .¹ ë

ä Ø 8 % ” o % ¾ î æ æ´ ! FIRST p´ N T » f P ^ ë „ , ì

APCERT ÿ o à ç d [# ¬ q CNCERT³ • æ´ d T™ # r , 0 D % Q !

Ù K t S , o % d õ ! P ^ < æ ! c³ • (S c h æ ! c J 0 c ! f ÿ K

³ • ä Ö 7 ! î æ -´]´ d

2 c æ `³

¹ Ñ ÿ £ ! § á d k S î æ³ < [— ° s n „ ð o í c ! ê

7´ ð o , Ä c - N S û ` ” b e c™ (ð r æ æ¹ Ñ ´ V³ d ½ ”

.¹ ¶ 0³ • ó æ´ d T) û ô l ä ð o k ° » f¹ ¶ ¬ (% c Ž ç c (• Ñ c

¿ ì³•ó î æ¹ÑqA •5Û Ÿ£ î^l Ýä î
æ¹Ñd

G>¹q!§ásP ôl‡W ~æÓeä•Û ðofÛ¬£ î æ
Ý ÓeG>c î æ¹Ñ Æã¹qc " î æqã _½Óe
æ*"b S î æ_½ðo¹qc î æ•iä‡Wðok° û`d

ë„%„!s ‘VŸ£ä ìp ½ Ö ¹ÑqA f"¹ëÉr~Ø8
%„ 7\$%„ ¹Ñgó!õ¹ S nû æ ¹Ñcĭf Ö³ S
¹Ñc•f7‘ÿ æ*ä7‘ðo,Ä ¹Ñc Ç4•N Öõ¹ ¹Ñ
»fBó³¥%„ë„l Ç4 R+ î æ¹Ñ d

Ë?y!´ î æ¿ c?y eæor Öq J³• û`€Vr
P• »³0 °¥cŸ³ Q cdp _gc_K ñn Ö-‘³y ÿ
æ*cr¹ææ*"b æ? û`d! ¹ð î æ-‘³y%G õ0(ð
ä S æ½ ,y³y ©% d

Í Ó C ² Á Ò ø

wCNCERT S æ ÝqAx »•ÅKqqAr ³¥™8o îë„,ì
%ø8Ø8/ï ÅK ³¥ S ë„/ï CNCERT g CNCERT/CC (•œ^
CNCERT©%Éú QãdqA/-«Ãgä • ^ , \{%ø cQãø-ëæ*
N d‡qAN ãFf ¶ CNCERT)û•8 #< CNCERT ½É åæ*g
Q â Ü‡qA»fc /• gÿg cP ïd
CNCERT Oú! ‡qA yòÿä¶-ÿ c/ ðoc ôlc Í+ 'bõ©
â´ ½Q g½rœ¬ æ... §l CNCERTâUä0®-' ø-¥Ð“ d

5F65 9 Ö

OBR ØL5B+ CNCERT Å6,5•¹~16ñ Ö z É È²ìØ)à\Ö z ^ X + ...L NÈ ÈB' Ø
ú & > A 6,3+ È• `pjÖ cncert@cert.org.cn Ä

Î Ã à ì ¶ Â Î Á ã ä

2022 ¼ 5 8 È Å6,,5•5•5 1~(æ å ¼ fAô ' j8ÿ Ä A - *.p5•
 5 F >| k f £0c È Å6,,5•PØ ø5• 4N©- #{ 7 7!" h ÈZ +OE³ W :
 5•5 1~ » & ÄX A - Å6,,5•5•5 1~)ß³ éM' ÈO XPœ F % h5•
 5 ì ?0; ç,´ IP ` p Gy Ã³ µ O XPœ F % h5•5 ì ?0; ç,´ IP
 ` p Gy ¼³ µ>Û = •>L,´5•1 Gy1yE³ : 8 9 p ÿ A È ì 42«
 5•5 1~ » & Gy w 9 = <0; Ö,´ Î Ð Ä

« Å E à ì ¶

2022 ¼ 5 8 È A - *.p5•5 F >| k f £0c È Å6,,5•PØ ø5• 4N©-
 #{ 7 7!" h È Z *)à-14x>| o j : ,´FP @E³ W ì ý,´ *.p5•5 F
 >| uLÌ È Z +OE³ W :5•5 1~ » & Ä

« » à ì ê È ¶

2022 ¼ 5 8 È i ž CNCERT,´- #{ ž ÈA - Å6,,5•5•5 1~)ß
 ³ k?± 7 7 õ å² ; Ö
 XPœ F % h5•5 ì ?#k Ø õ å éM' È³ µ4Ö 478 7 Z IP ` p) Ä
 ,´ k j>Û XPœ F % h5•5 ì ?0; ç x f ÈE³ : 8 ÿ A 5.7%Ä
 0+ Ø Å6,,5• ì ?0; ç éM' È)à øAø 3R2« ì ?0; ç g \ 54 Z Ä
 CNCERT A Ä+X v Ç ÄZ ê5•1 Ä¯ z £ ÄÁ £ 1y P Ý\$PFfFJ Ö
 ; æ0+ Ø Å6,,5• ì ?0; ç 1,263 Z È 9>| j Ž W5 AÑ È WG 6 jB!PÇ
 !jAø2« Ä

5•1 1~ éM' È ³ µ>Û2 i5•1 Gy j 5,279 Z ÈE³ : 8 ÎK¯ 4.5%×
 ³ µ>Û = •>L,´5•1 Gy j 1,838 Z ÈE³ : 8 ÿ A 21.4%ÄJ,)³
 µ5•1 ,´ / ÄN¥M' Gy j 16,540 Z È#¹ ú = 15,834 Z ÈP ` p 586
 Z Ä

1~%?#N éM' È \ 8 CNVD ì fLö ¼*6 Ý3+5 1~%?#N 1,548
 Z ÈE³ : 8 Î Ð 14.9%Ä ! jQ ì %?#N 546 Z ÈE³ : 8 ÎK¯ 26.4%×

>Û Y+X • Î íF 0; k +, '%?#N 9 1,274 Z ÈE³ : 8 ÎK⁻ 14.0%×M&
%?#N1,162 Z ÈE³ : 8 ÎK⁻ 40.7%Ä 9%?#N2« » 6 3 Â = } 9 },'
6 [_ WEB Ä+X%?#N Ä Ä+X0; ç%?#N ¼5•5 Aî 7%?#N Ä
» & *6 éM' È CNCERT Õ f `5•5 ¹ ~ » & Õ z 11,638 & ÈE³
: 8 ÎK⁻ 17.9%È Gÿ 0 J, ' 6 [_%?#N2« » & 3,700 & Ä ! ?0; ç
2« » & 3,648 & ú5•N¥ / Â2« » & 3332 & Ä
» & 4*6 éM' È CNCERT 4*6 ¶5•5 ¹ ~ » & 11,642 & È Gÿ 0
J, ' 6 [_%?#N2« » & 3,709 & Ä ! ?0; ç2« » & 3,640 & ú5•N¥ /
Â2« » & 3349 & Ä

_ !Ù & 1 & (57 ç N â s A M + 1 Ñ ä ÷ m Ñ + 1 Ñ q A) û % " f # ³ Ä ™ ds ÷
m Ñ ¹ Ñ q A & 1 & (57 g / ³ S Ø V ± ÷ m Ñ / ï % " d

• y Ð § † K

z ð o, Ä

ð o, Ä ¾ ™ 8 o ÷ Ñ c (Ñ c î ä ¹ ð •• ! N » % 8 ð o ä

ô l , , Ä d

z ° S

° S ¾ ð o, Ä / (Ñ c ÷ Ñ g ¹ ð Ø Ð / É } î a g â Á ò "

¶ — ¶ ° ^ l à } # Ñ ã Æ ã • À 9 g E * , Ä ý ! ð o, Ä K , æ ä ç d

z • É Q

• É Q ¾ } # < Ñ ã Æ ã • } ð o, Ä / m c û » Ò p â p ò

, Q d • É Q Ó + \ " • !

1. < î " • ô Trojan Horse

< î " • ô Å K • ô ¾ » Ü Q ð o Ž ¾ Y Q Å %

™ 8 o V ' , • É Ý ò d Q ¾ • > ç , Ž & (— 0

¾ ú / q • ô r ¾ î ¥ Ó - Ù — ` • ô d Ö _ ÿ • ô Q

¶) ç ä Ó ! Ü • ô ² c ß • ô ³ c ± A • ô ⁴ c Y Q Å % • ô ⁵ c

h [• ô ⁶ c • { à • ô ⁷ ä c Q • ô ^ + d

2. Ú £ Q Bot

Ú £ Q ¾ r Ù Ö Ÿ f ^ l < [• É Ý ò d Ö ° ¹ ð Ø Ð

Ú £ Q ¶) ç ä Ó ! IRC Ú £ Q c Http Ú £ Q c P2P Ú £ Q

ä c Q Ú £ Q + d

3. k Worm

k ¾ Ÿ ' A % ä œ • Ž ì » ½ , Ä ä î † W V ' ,

• É Ý ò d Ö Ž ì i E k ¶) ç ä Ó ! Ñ k c † " È o

k c U í k c ° S F k ä c Q k T + d

_ ! Ü • ô ¾ ± Ü (• ± c î „ ì Ü • ô d

_ ! ß • ô ¾ ± Ü ß c ê ì Ü • ô d

_ ! ± A • ô ¾ ± Ü V o / Y + 3 Ñ g ô l • ô d

_ ! Y Q Å % • ô ¾ » â p ò í m f V o • 8 T ä « É Ÿ t ¹ ¶ î Å V o • ô d

_ ! h [• ô ¾ [î - h p ^ l à G ç \$ • ô d

_ ! { à • ô ¾ • { W • • É Ý ò p V o É n û ») ç ä Å V o • ô d

4. È] Virus

È]¾¹¶+ù™8o3Ñ)ûŽÌ »E*g¾ ôl ð¹ð
o,Äp(nû V', •ÉÝòd

5. cQ

híÓ+#gÃ cQ•ÉÝòd
; ,ñ° •!æ] Ÿ° S h{£ çÔ•ÉÝò.n hí
Ó+ / •7_Ÿëÿä•ì<\$ ÉânŸ°ds® A,Ü Ö•
ÉÝò V' İöÖhíGì)ûç+d

z Ú£ î

Ú£ î¾,ñ° ,/Å%™8oö câì<\$¾ñ°Ÿt¹¶çs•
a—0Å%ð š+ù•ôgÚ£Q Vo û-½ •Éû "¶½
"sv,³ ç)ûÓã´k‡û`^l gŸ"Öh ÷m Ñ g)ûqë
àr d

z k‡û`^l

k‡û`^l¾çvç,³ðo,ÄŸ"A, ^lg g û<G^l
´ »Y!°,³,Ä´ "bû`d

z š¾

š¾¾•ÉE*gW š• ° çM¥p(]´g{£ñ° &
Äp(š• d

z šç

šç¾¹¶r•0vç,³ ç:g- šK ,K7(ç É
¹(»÷m Ñc‡"mŸcíokðg š ñæA °´Ÿ"Kÿ´ „
ç or Z,ÿÈo , À97(ç »fÜ Q =Aðo "
ßûËÜäË Aò d

z š<ô

š<ô¾¹¶} š/"&•ÉÝòg] !°™8o}À9 š
K"„ &•ÉÝòd

z ç*

ç*¹Ñ¾ñ°} ç <G,Ã/hŽYQÅ%šK¶—Ÿt¹
¶ šK=AYQÅ% çû`v ^l¹Ñd

z ÷ m Ñ
÷ m Ñ¾ Ü â ‘ È o ¹ (¾ # < È Ð œ A ÿ " S 9 • ì Ñ d
g ó ! ç ì Ñ ¹ • " { ‘ Ð g à ½ É ì œ A c (• œ ^ c R 5 ù
´ & Ž 6 & Ž ŷ (• Ñ " • ì Ñ M ≠ k ì (• Ñ " 8 â ŷ
ÿ Ñ † Ú c c³ • ð o (• Ñ " Ñ ÷ ð o W c ÿ Ñ c
¾ ð o (• Ñ d
z 7 ` [7 ` [¾ ¹ ¶ 7 ` e È Ð g¾ 7 ` û ` v h ô l ° }
À 9 - ‘ 7 ` ¨² M ÷ IP g ° È Ð ž G d
z Ä Ñ ã À 9
Ä Ñ ã À 9¾ À 9 ã « » Ä þ ò Í m À 9 ô l ð o d Ä Ñ ã À
9 ¹ Ñ ç N Ÿ “ } É } ° S ð o , Ä / ñ ° F e * ° S F Q
Exploit ŷ f Ü ð o , Ä À 9 ã « d
z - N S • É Q
} â Æ g # Ñ ã Æ ã • } - N 4 j , Ä / m c n û » Ò þ â þ
ò , g n ±³ ¥ - ‘ ¥ Ð ¥ Ÿ û ¶ û 3 Ñ c Q f Ö g Q + m d