

Firmware Security Audit Report

NYARC - Nyarime Advanced Reverse-engineering Console

Nyarc Professional v1.2.0

Firmware	4.0.24 x64 Build202601131850
Vendor	iKuai
Sample	iKuai8_x64_4.0.24_Build202601131850.bin
MD5	4fa9b7183ae1cc505295dc4ef5f5afbf
SHA-256	1bee8284ee70f633b8b88bd6bbbfc7a366f9b01f1700dac83b35171fa8b9fb63
Size	41.7MB
Scan Date	2026-04-22 23:22:04 UTC
Tool	Nyarc Professional v1.2.0

RISK SCORE: 56/100 (MEDIUM)

Findings: 18 Critical, 12 High, 5 Medium, 528 Info

UNLICENSED EVALUATION COPY - NOT FOR COMMERCIAL USE

Findings Overview

#	Severity	CVSS	Finding
1	CRITICAL	6.9	Password cracked: user 'root' (2x)
2	CRITICAL	5.3	OpenSSL libcrypto.so.1.0.0 - EOL
3	CRITICAL	7.5	OpenSSL 1.0.0 - EOL
4	CRITICAL	9.1	Private key leaked: /etc/remote2/ca-certificates.d/ikuai/client.key
5	CRITICAL	9.1	Private key leaked: /etc/ssl/32015/ca.key
6	CRITICAL	9.1	Private key leaked: /etc/ssl/32016/ca.key
7	CRITICAL	9.1	Private key leaked: /etc/ssl/32017/ca.key
8	CRITICAL	9.1	Private key leaked: /etc/swanctl/ikca/rootCA.key
9	CRITICAL	9.1	Private key leaked: /usr/ikuai/ctrlclient/priv.key
10	CRITICAL	9.1	Private key leaked: /usr/openresty/ssl/server.key
11	CRITICAL	9.1	Cloud control client: private key + certificate leaked
12	CRITICAL	6.1	Control client (alt): private key + certificate leaked
13	CRITICAL	9.1	Embedded CA: private key + certificate leaked
14	CRITICAL	9.1	Embedded CA: private key + certificate leaked
15	CRITICAL	9.1	Embedded CA: private key + certificate leaked
16	CRITICAL	9.1	Web server: private key + certificate leaked
17	CRITICAL	7.5	OpenSSL 1.0.0 - End of Life
18	HIGH	5.3	Generic backdoor detected (CVE-2023-50920): Lua random seed (check for predic...
19	HIGH	5.3	Generic backdoor detected: JSON parser library (sscanf overflow CVE in parse_...
20	HIGH	5.3	Generic backdoor detected: JSON parser library (sscanf overflow CVE in parse_...
21	HIGH	5.3	Generic backdoor detected: JSON parser library (sscanf overflow CVE in parse_...
22	HIGH	5.3	Generic backdoor detected (CVE-2023-50920): Lua random seed (check for predic...
23	HIGH	5.3	Generic backdoor detected: JSON parser library (sscanf overflow CVE in parse_...
24	HIGH	5.3	Generic backdoor detected: JSON parser library (sscanf overflow CVE in parse_...
25	HIGH	5.3	Generic backdoor detected: JSON parser library (sscanf overflow CVE in parse_...
26	HIGH	5.3	Generic backdoor detected: JSON parser library (sscanf overflow CVE in parse_...
27	HIGH	5.3	Generic backdoor detected: JSON parser library (sscanf overflow CVE in parse_...
28	HIGH	7.5	Remote control configuration exposed
29	HIGH	5.3	Generic backdoor detected: JSON parser library (sscanf overflow CVE in parse_...
30	MEDIUM	5.3	User 'sshd' uses MD5crypt weak hash (2x)
31	MEDIUM	5.3	User 'root' uses MD5crypt weak hash (2x)
32	MEDIUM	5.3	Generic potential vulnerability: Telnet on non-standard port (potential backd...

Detailed Findings

NYARC-001 | CRITICAL | CVSS 6.9

Password cracked: user 'root'

Description: Password '2015.ikuai8.com' found via dictionary attack
Evidence: /etc/shadow: root cracked with common password dictionary

NYARC-002 | CRITICAL | CVSS 5.3

OpenSSL libcrypto.so.1.0.0 - EOL

Description: OpenSSL 1.0.x is EOL since 2020, multiple known CVEs including RCE
Evidence: /usr/lib/libcrypto.so.1.0.0

NYARC-003 | CRITICAL | CVSS 7.5

OpenSSL 1.0.0 - EOL

Description: OpenSSL 1.0.x is EOL since 2020, multiple known CVEs including RCE
Evidence: /usr/lib/libssl.so.1.0.0

NYARC-004 | CRITICAL | CVSS 9.1

Private key leaked: /etc/remote2/ca-certificates.d/ikuai/client.key

Description: Private key found in firmware. Anyone with the firmware can impersonate this service.
Evidence: Private Key: /etc/remote2/ca-certificates.d/ikuai/client.key Certificate: /etc/remote2/ca-certificates.d/ikuai/client.crt subject=C = CN, ST = beijing, O = ikuai, OU = ikclient, CN = *.ikuai8.com issuer=C = CN, ST = beijing, L = bj, O = ikuai, OU = ik, CN = *.ikuai8.com notBefore=Aug 22 09:52:29 2019 GMT notAfter=Aug 19 09:52:29 2029 GMT serial=02 SHA1 Fingerprint=FB:07:C4:91:0E:A9:26:86:98:4D:EE:CB:33:A1:8C:B6:E1:F4:B3:2F

NYARC-005 | CRITICAL | CVSS 9.1

Private key leaked: /etc/ssl/32015/ca.key

Description: Private key found in firmware. Anyone with the firmware can impersonate this service.
Evidence: Private Key: /etc/ssl/32015/ca.key (1024-bit RSA) Certificate: /etc/ssl/32015/ca.crt subject=C = CN, ST = BeiJing, L = BeiJing, O = iKuai, OU = iKuai, CN = download.ikuai8.com issuer=C = CN, ST = BeiJing, L = BeiJing, O = iKuai, OU = iKuai, CN = download.ikuai8.com notBefore=Aug 29 04:13:19 2017 GMT notAfter=Dec 30 04:13:19 3016 GMT serial=BD9552A22264C655 SHA1 Fingerprint=68:7C:26:F4:B4:20:1B:C5:04:AD:31:58:0E:4F:C1:04:08:6C:39:B6

NYARC-006 | CRITICAL | CVSS 9.1

Private key leaked: /etc/ssl/32016/ca.key

Description: Private key found in firmware. Anyone with the firmware can impersonate this service.
Evidence: Private Key: /etc/ssl/32016/ca.key (1024-bit RSA) Certificate: /etc/ssl/32016/ca.crt subject=C = CN, ST = BeiJing, L = BeiJing, O = iKuai, OU = iKuai, CN = download.ikuai8.com issuer=C = CN, ST = BeiJing, L = BeiJing, O = iKuai, OU = iKuai, CN = download.ikuai8.com notBefore=Aug 29 02:15:37 2017 GMT notAfter=Dec 30 02:15:37 3016 GMT serial=92EDE68AEB529720 SHA1 Fingerprint=B8:4C:CB:B7:53:F6:70:9E:B8:D8:20:DB:8A:34:49:BE:85:E8:30:F0

NYARC-007 | CRITICAL | CVSS 9.1

Private key leaked: /etc/ssl/32017/ca.key

Description: Private key found in firmware. Anyone with the firmware can impersonate this service.
Evidence: Private Key: /etc/ssl/32017/ca.key (1024-bit RSA) Certificate: /etc/ssl/32017/ca.crt subject=C = CN, ST = BeiJing, L = BeiJing, O = iKuai, OU = iKuai, CN = 302.ikuai8.com issuer=C = CN, ST = BeiJing, L = BeiJing, O = iKuai, OU = iKuai, CN = 302.ikuai8.com notBefore=Sep 6 04:04:56 2017 GMT notAfter=Jan 7 04:04:56 3017 GMT serial=E43325EF748B108B SHA1 Fingerprint=EC:29:58:77:4B:E1:99:CC:DA:74:14:A2:B9:0B:D9:D7:EF:C9:D5:36

NYARC-008 | CRITICAL | CVSS 9.1

Private key leaked: /etc/swanctl/ikca/rootCA.key

Description: Private key found in firmware. Anyone with the firmware can impersonate this service.

Evidence: Private Key: /etc/swanctl/ikca/rootCA.key (4096-bit RSA) Certificate: /etc/swanctl/ikca/rootCA.crt subject=C = IK, ST = beijing, L = beijing, O = ikuai, OU = ikuai, CN = ikuaitest.com issuer=C = IK, ST = beijing, L = beijing, O = ikuai, OU = ikuai, CN = ikuaitest.com notBefore=Dec 27 01:59:58 2022 GMT notAfter=Feb 25 01:59:58 2042 GMT serial=A1142FC16A202365 SHA1 Fingerprint=A4:86:5B:9B:F1:6F:66:AF:01:B3:EE:9B:A4:90:90:56:60:DB:2A:7E

NYARC-009 | CRITICAL | CVSS 9.1

Private key leaked: /usr/ikuai/ctrlclient/priv.key

Description: Private key found in firmware. Anyone with the firmware can impersonate this service.

Evidence: Private Key: /usr/ikuai/ctrlclient/priv.key (4096-bit RSA) Certificate: /usr/ikuai/ctrlclient/cert.pem subject=C = CN, ST = BEIJING, O = IKUAI8 Ltd, OU = CERT 0001 OF CA REMOTE CONTROL 0002-01-0001 FOR IKUAI ROUTERS, CN = cert0001.rm_router0002-01-0001.ikuai8.com, emailAddress = admin@ikuai8.com issuer=C = CN, ST = BEIJING, O = IKUAI8 Ltd, OU = REMOTE CONTROL 0002-01 FOR ROUTERS, CN = remote_control.rt0002-01.ikuai8.com, emailAddress = admin@ikuai8.com notBefore=Dec 24 02:44:23 2015 GMT notAfter=Dec 22 02:44:23 2021 GMT serial=100000 SHA1 Fingerprint=9B:3C:A3:86:B7:65:80:CB:A8:B4:BA:77:8B:B8:53:B4:84:99:6A:2B

NYARC-010 | CRITICAL | CVSS 9.1

Private key leaked: /usr/openresty/ssl/server.key

Description: Private key found in firmware. Anyone with the firmware can impersonate this service.

Evidence: Private Key: /usr/openresty/ssl/server.key (2048-bit RSA) Certificate: /usr/openresty/ssl/server.crt subject=C = CN, ST = BeiJing, L = BeiJing, O = iKuai, OU = iKuai, CN = ikuai8.com issuer=C = CN, ST = BeiJing, L = BeiJing, O = iKuai, OU = iKuai, CN = ikuai8.com notBefore=Apr 21 07:23:05 2021 GMT notAfter=Aug 22 07:23:05 3020 GMT serial=DB6C3FFC850ABE5E SHA1 Fingerprint=45:EF:86:D9:14:1C:AC:5B:45:CB:02:FD:BB:95:5B:75:5E:01:A3:EE

NYARC-011 | CRITICAL | CVSS 9.1

Cloud control client: private key + certificate leaked

Description: Private key and certificate pair found in firmware. Any attacker with the firmware can impersonate this service.

Evidence: Private Key: /etc/remote2/ca-certificates.d/ikuai/client.key -----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED DEK-Info: DES-EDE3-CBC,F0E01D1AC88DB129 TsoiD/A5nDgSA2zLX4rX8iSIV2KwmCgr2Ov8h3hDI+FFsdYu63/Lhf74YS50LJ/4 b0jaljXLZ3tg1usincorTxZEz+i7C6/qOYsch7KTVNk1JTQ6hwlmrZhyNIs4vgi tKT8rLnPzkW5qLm0nbdjPHXeGt8SxH/yefAKWpQo6vwH2+DD6YHJ/haprRd2Mqr5 3mRnfHe1TodaWdO+td6VBd3RND3kVCyF/uUBwhIH9IXRq4benqHIJATq4U/QymMC AoxHXFi389K45/Ck8XMxcz84+ESmjZLyVEsS66D1GyyVqoe0B6y4e+aQnE28cFMZ +oHPWRfbFHGtWeRw/n0fo8DVx5BSrfoO3I2/WIDLsMbK+s5EkN8Q974nDhqZQMP4 tc0efp4qNjhTichkSpalErS0Ws1hEnILMUxR+3bsjgl9E+4nfE9dEad79L9evkds /ywPC32x6FWVjGxTy1IT5gUVw4U++WKf2oj7IUh+39qEXjOd2IRMZer0/21EWR2 ep1Fp7fm2jRF74fiiB91Mugh2AEhG0dgOPQucvnyh/wahKRwdTUBxtnN2EKhN4qx FO79S2s0B6+rDuLvj3+tg5bPPIme1/n8l78qnLwnH93f9WxWsRwxnE4MwOeP+Fj aozRwxX6jOapEhpMSK0J0rNCi+bH+bupDbm17WWddeseqkJeFplGEcJ5BfzVZER n20GAtELoAA6jg9JR8piVQw2LC/RB6zaOO/GCid6My1tYnn5deXpRIKCEru+mH58 9oQ2oMxy3akJ3nFo/fBpTGyMkqye6jhrUQ9XYTNU3lubavGmpFwVZQ== -----END RSA PRIVATE KEY----- Certificate: /etc/remote2/ca-certificates.d/ikuai/client.crt subject=C = CN, ST = beijing, O = ikuai, OU = ikclient, CN = *.ikuai8.com issuer=C = CN, ST = beijing, L = bj, O = ikuai, OU = ik, CN = *.ikuai8.com notBefore=Aug 22 09:52:29 2019 GMT notAfter=Aug 19 09:52:29 2029 GMT serial=02 SHA1 Fingerprint=FB:07:C4:91:0E:A9:26:86:98:4D:EE:CB:33:A1:8C:B6:E1:F4:B3:2F Certificate: Data: Version: 3 (0x2) Serial Number: 2 (0x2) Signature Algorithm: sha256WithRSAAEncryption Issuer: C=CN, ST=beijing, L=bj, O=ikuai, OU=ik, CN=*.ikuai8.com Validity Not Before: Aug 22 09:52:29 2019 GMT Not After: Aug 19 09:52:29 2029 GMT Subject: C=CN, ST=beijing, O=ikuai, OU=ikclient, CN=*.ikuai8.com Subject Public Key Info: Public Key Algorithm: rsaEncryption Public-Key: (1024 bit) Modulus: 00:ee:90:43:48:da:3e:77:10:23:4d:54:b9:95:47: 4b:00:31:74:51:7b:55:9d:0c:f2:98:2e:00:e3:1c: 56:03:fc:56:97:d5:23:5c:f5:12:32:42:4f:b0:de: 24:1c:73:10:d7:a1:ca:6d:34:23:f1:10:f7:ad:34: a2:1f:3d:b7:76:9a:4a:03:51:cc:e5:5b:e9:ee:c2: d2:0e:23:11:4c:b6:ff:cb:41:8f:1d:85:ac:5d:58: ce:07:24:ce:de:8f:22:af:13:7e:5e:10:a5:4c:e0: 0b:d5:03:a4:9d:79:e5:bb:e2:5e:1e:7b:43:da:d1: e5:c0:0a:0e:cf:b5:5a:a2:17 Exponent: 65537 (0x10001) X509v3 extensions: X509v3 Basic Constraints: CA:FALSE Netscape Comment: OpenSSL Generated Certificate X509v3 Subject Key Identifier: 71:9A:96:1A:11:92:1D:83:F7:C2:EE:17:1C:D1:DE:DF:BA:D9:8F:92 X509v3 Authority Key Identifier:

DirName:/C=CN/ST=beijing/L=bj/O=ikuai/OU=ik/CN=*.ikuai8.com serial:FB:BD:09:09:DE:43:08:9B
Signature Algorithm: sha256WithRSAEncryption 38:ac:b9:fd:1f:b5:65:08:c9:3a:d8:69:df:e3:b3:56:46:1c:
47:4b:8e:07:09:12:57:aa:da:34:67:dd:32:cf:f7:45:b7:a3:

5e:37:11:c2:ed:26:f6:a9:b9:c8:ac:52:e5:c2:e0:38:1c:25:
81:2c:da:81:38:e4:d4:27:c3:7c:90:dc:b1:39:8a:f7:59:ba:
0b:1b:f6:76:07:b4:5c:01:9c:68:d3:52:51:08:d9:3d:f5:1c:
08:7d:64:1f:6d:85:0e:3a:1c:73:35:8d:52:8d:c1:9d:ad:92:
75:2f:5c:13:1a:9c:42:16:8e:52:53:36:6c:9f:af:9e:dc:56:
37:09:a6:43:1c:b7:30:d0:34:65:b9:a4:a0:6c:e6:b5:7e:23:
43:9f:00:92:01:58:d9:e7:7d:33:30:3e:c0:7f:8e:66:72:d8:
5c:11:b6:d5:0e:39:24:d3:4f:79:d5:37:b2:f8:13:75:ea:f1:
20:66:34:cb:e7:eb:12:cc:e0:35:3e:fb:c9:e8:c7:86:5d:33:
9d:55:d1:f0:1a:89:2c:93:ba:6f:e4:79:fb:f8:35:3a:41:a8: f8:94:7f:55:a5:bf:0d:27:04:5e:31:fa:74:72:cf:af:8c:3f:
08:e5:f9:ed:c3:cb:fe:a8:f7:67:83:0a:8f:43:cd:22:bb:7d: bc:0d:b7:c2 -----BEGIN CERTIFICATE-----
MIIDiDCCAnCgAwIBAgIBAJANBgkqhkiG9w0BAQsFADBgMQswCQYDVQQGEwJDTjEQ
MA4GA1UECAWHYmVpamluZzELMAkGA1UEBwwCYmoxDjAMBGNVBAoMBWlrdWFpMQsw
CQYDVQQLDAJpazEVMBMGA1UEAwwMKi5pa3VhaTguY29tMB4XDTE5MDgyMjA5NTly
OV0XDTE5MDgxOTA5NTlyOVowWTELMkGA1UEBhMCMQ04xEDAQBgNVBAgMB2JlaWpp
bmcxDjAMBGNVBAoMBWlrdWFpMREwDwYDVQQLDAhpa2NsaWVudDEVMBMGA1UEAwwM
Ki5pa3VhaTguY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDukENI2j53
ECNNVLMVR0sAMXRRe1WdDPKYLgDjHFYD/FaX1SNc9RlyQk+w3iQccxDXocptNCPx
EPetNKIfPbd2mkoDUczlW+nuwtlOlxFMtv/LQY8dhaxdWM4HJM7ejyKvE35eEKVM
4AvVA6SdeeW741ee0Pa0eXACg7PtVqiFwIDAQAB04HXMIHUMakGA1UdEwQCMAAw
LAYJYIZIAyb4QgENBB8WHU9wZW5TU0wgR2VuZXJhdGVkIENlcnRpZmljYXRIMB0G
A1UdDgQWBRRxmpYaEZldg/fC7hcc0d7futmPkjB6BgNVHSMeczBxoWSkYjBgMQsw
CQYDVQQGEwJDTjEQMA4GA1UECAWHYmVpamluZzELMAkGA1UEBwwCYmoxDjAMBGNV
BAoMBWlrdWFpMQswCQYDVQQLDAJpazEVMBMGA1UEAwwMKi5pa3VhaTguY29tggkA
+70JCd5DCJswDQYJKoZIhvcNAQELBQADggEBADisuf0ftWUlyTrYad/js1ZGHEdL
jgcJEleq2jRn3TLP90W3o143EcLjvupucisUuXC4DgcJYEs2oE45NQnw3yQ3LE5
ivdZugsb9nYHtFwBnGjTUIEI2T31HAh9ZB9thQ46HHM1jVKNwZ2tknUvXBManEIW
jJTNmyr57cVjcJpkMctzDQNGW5pKBs5rV+l0OfAJIBWNnnfTMwPsB/jmZy2FwR
ttUOOSTTT3nVN7L4E3Xq8SBmNMvn6xLM4DU++8nox4ZdM51V0fAaiSyTum/kef4
NTpBqPiUf1Wlvw0nBF4x+nRyz6+MPwjl+e3Dy/6o92eDCo9DzSK7fbwNt8l= -----END CERTIFICATE-----

NYARC-012 | CRITICAL | CVSS 6.1

Control client (alt): private key + certificate leaked

Description: Private key and certificate pair found in firmware. Any attacker with the firmware can impersonate this service.

Evidence: Private Key: /usr/ikuai/ctrlclient/priv.key (4096-bit RSA) -----BEGIN RSA PRIVATE KEY-----
MIIEKAIBAKCAgEA9QQ1rQPfV15bMoOYdZqzNz1Sb77M0agE+VSm63KIC1J73MSc
VJZ+2tQE8ro8zgzShhvUgZcKtqzZeNjUA9N/6yBVQdOBRh/Bj4FizY8IOvYt1z
a35gGZW7EsMfmhsQ0JKEih1i2JW0riWvh6h60dIKslPbd6Dleb3ViNWtjUC13t
NqTiFb3gMyNcl72354fFbcWRKANNk7EFVuz35DRqaRRDtyJ/KOskyYBSCZO1/tE5
vIwFeQgUBZBL9ksw0TNS7esHdg9OoLLRezt44lpHe7xqpH23/Yc0d/oYS4CsCHY1
LkE/Z69fjY2vo2+SKDTSit9chcRWpifznZetY5Mnlcd93qS5mGCfjx4AcyvmXoQx
KfN1A9pnm2XWxWs0MMLK1xlyvjxn3pbSpF/Cj7WUx3NBAuCIK7PvRt7d+tu+6MuY
S4UdzGwL1isseOYQ4y00SiQLmus/y1iFiQ/nf+MRZd+yK4adDcj6fQsXRNRbtLX
dG2friGi99TOft914zVH733ZRvfv+0OOecynU198bvGh23ecNp/CMymYCKhi+Joi
h77Bdm+mZ7GUwbPJ63MJJhqbKppwNBVDblAzejOmwhLtvSPxkpu49MmtRADMu8U
BfDvZspV44cileZtV/w41votilpE9puJsde7HcNuouz2v9WHxyM6J2H1+IUCAwEA
AQKCAgEA1xAT4ULV5aS63fL+frQEfQc5ddZ/R8P4YbX5Mg+WaQLER/pv0hurS37w
vPHV72vHMImOwtpTlJnPth7Pg92QHrdUITM81n2lqDdugfNDdikYeGozJnZt+ecg
po5ZddaWAs2owuaaXcvCJV303d3vPZl5zOOH0okzh6c56HrOfFsZnHShrVhsX3R
7nEqLkEXzIWzOPBCwmFr1ah7LFqiGFAd2xArgyPleq0zxB77Y2ahSAL0cW+qahs6
H8wRsSU8kTJQp382NF2pQv44fdl2abmqeivnqSvPD1SQ8FIU9ikqGTBt1EUS3l3
IOw/wDBtlRcQe08IkIDM9o/w2TJKwLWrlFdvofkHMHsmz2hMQooRupsqo6nm7yG
JGYXteVfpJaw+nUpHUPWM9+7ax/kovj6ioVLoEn8ZhSD3eo+EzsXb7UWXCQwiqj
VZYwaOH0/6jnrDg1hbOZbGwiBBx9fplf18PwZ+mMXTHdhagMIMzRB+UxvJ1aqzt
AgJRq+9PIvqE5/QofS7WJjPMkCyFICva0WGxsWcE004gwN2TJ4owsSSLq2MB10uM
omWHUur0Br+2VN1i1+9maHy6m534aOO9damPTgkku3XMHJAI+YTzvyvmAJm3l+uX
e5ByjzKRv7tZ9Knrwb5bMp5pTDiGnYmwSIPUAi6Vwmvlgjp8ECggEBAP8l88tw
3/AHykGnGctopNob8M/Ypy22Hosymtsg79MFc28ysl2TIBk69blH2lF2TkwE9/VZ
aRP/YHGuxxMy1rgFQuVl4OIFIID/y0dA4PzpOBQ3Yhjn2ZWekro3zjV2aZ6T38Mk
2GJkH034JdUCOR7d5RQ4pGzpz+BGhkR+1oGUaOwZMXEJjVXniOYYvhXhDWagm
iXMJl06QAIHlUjPk/fzAoH5BXOjTgUg0CixQJmNZ+pe5jLleGwbK31YkH++4FT1N
5uzqd+ADS/z6hL/WvFaKd6xgxpIgzRqQu6vjo4j+dviJZNIjmNzyQAqBjDCplf08

HAYDVQQDDBVydDAwMDIucGtpLmrdWFpOC5jb20xHzAdBgkqhkiG9w0BCQEWEGFk
bWluQGlrdfWFpOC5jb20wHhcNMTUxMjI0MDIzMTMyWhcNMjUxMjIzMTMyWjCB
sDELMaKGA1UEBhMCQ04xEDAObGVBAGMB0JFSUpJTkcxEzARBGNVBAoMCKILVUFJ
OCBMDGQXkZApBgNVBAsMIJFTU9URSBDO5UUK9MIDAwMDItMDEgRk9SIFJPVVRV
UIMxLDAqBgNVBAMMI3JlbW90ZV9jb250cm9sLnJ0MDAwMi0wMS5pa3VhaTguY29t
MR8wHQYJKoZlHvcNAQkBFhBhZG1pbkBa3VhaTguY29tMIIcIjANBgkqhkiG9w0B
AQEFAAOCAg8AMIICGKCAgEAWYBgUKTWOwz0j+sE6xC3HBIADJRH8a4Gq/fcuGML
+I2SqbeDOAT95PFwCptDkFVx7Aqs6NVirVm80XOFp23R+ZCzXYtcNfcZ1JsfIEgB
oZPyEjoCkU7kVoRC0yti+3Ay4sRh4+I702LZWDYQHfVkc3bRiHKs8rUIPiSST4It
r0WHnKXBmDX+jOqMd0vhqf2iYHZ9KR4BNSbdW+pEFdGmluC5UIBoZGikWC8+x/
WpB6uPR3rp3x3EcPdUYeF1xe64TFZDg62cdvxAMXSEvSj6XWYN37CQnUBzDRY4jP
db1SoZQ041QTIVZ2Ng1U0pjEccinOnxznYyluT3hkhdMS1tkLHqY7YrFIYhSKxy7u
Yapm5b5m9FG8b9P8TRZbwK9P1gby//OLufz1CZ9TZh1Gao4ha1CkHKL7r9Bqm8FU
pmLOGAbmCLnIDcD61iVJfkomU1fHl5Cpv4Cgzhq7nqngAcG4uxshLasKvTEnltr
mQ85yhkD5TzTxGyJDM7ruff8fURSxoPu7QMdfnLfhwizMTf7RwsHjvGVX0xDjHG
X+41/Fwb9UmFZUXBx9LU4kEEiToM0Oj/tfz1KN3Y4uTtaogVdYoBeQEtzynaRFJk
2nj4oYL7bhJEI4PKwEzWILNKXcqkOfDNE+F1jBPUN3VyCEm3EhYkCZUHTKnFGQJ
UUsCAwEAANQME4wHQYDVR0OBBYEFMyp0r9IX2v0B6BWtmVw85u6SQ/BMB8GA1Ud
IwQYMBaAFDhs+J6vp0Pn57q4/Gk6iqjAn0UMAwGA1UdEwQFMAMBAf8wDQYJKoZI
hvcNAQEFBQADggIBAEEmNEDAwQI0coYE0JmjgZGwSnes0Gi2BPRMR4/2ZPA5MBQ55
C3Otk+Clrw/zcUz4TX87q1Mx0wn263VrV9Dq6qkric3OV7430LGgva0GW3IS7/3N
zo3t9jMw/OULM+IgsW6ADjHWv4c0JGJ+f+fzViqKagOI7uVWEXpQ1mHZIYN03rrs
mE+jG2T448QeNXYJE4R6KQ2CxDO9VzzD83eAJktZetZt4B+3JDTp/2zwq1bPsvXZ
3gO7N+JYSqL2DF28Y/4xSrbS9Kp9fUeX/IpT//iMkCMjrlppU9CxCs9cTJ+s6v8
Y1CZDuaPQYqeX5nDhkmslCV6vITzLi3Odu0ewLqpaw23ew7I9NrOkVy77zR2PP
PFU8xh5S7S+sHxYuW4/oBjLk7O8hvH0edHD/NVIZpL9FfsP1DbH9VnPL6fg8iitr
p0cMRfby2r+pFweJhNCRpU7e+I5dT264rFgxLZ9SHP2j3QDfIgiE+Ccjpp+zIB2
5Wz5hsZf/YE0O3AEREh+VBOOKcTcyFnEqbrBCg4sUofxTRpurJ17GNLhOASJH+fc
Jc12dfOzWkIz0sKfjMni+g0NFT05BW5UaFC0MXd0qRzmyP4eq/AZu9V3cTsUQxdx
ALPPSRRAhSfDHmx7sHiTHlJijqytKvsm6bJDJoT/MRdlitV+Udk9UZhYczPK -----END CERTIFICATE-----

NYARC-013 | CRITICAL | CVSS 9.1

Embedded CA: private key + certificate leaked

Description: Private key and certificate pair found in firmware. Any attacker with the firmware can impersonate this service.

Evidence: Private Key: /etc/ssl/32015/ca.key (1024-bit RSA) -----BEGIN RSA PRIVATE KEY-----
MIIcXAIBAAKqGQCkw28LFzV00+SWY1kpVrxmz1uRT7L5wZyh3VzJB6ZuqNcthhN
efu/CsPUkV6rH0IDqdbIcLmMwFS4XOea5XA+QFIEjhh5tHuZ18FLsKwwB4DRXv9T
Irkpbh1ijzS98INSP5qIMjIHBmnNeeV96UTQvrhu5p0XVS2l1qRuFiJdQIDAQAB
AoGAHid+2PvafsmvdRbGBsIWXdxDCU/aAYhamYR4kkIA0JAHBfYZAEgsrdtwxgS0
aRTWti9y9pIglCvli/aRtuon2LDt0iAJMn8LkvmjPyLyvET4zOsZ8/liqOILyv8E
cjpVbnjexsWZhCiTi0AkUBNaKKrjeywxuChgCW6JIOTOqECQQDi6P+Y8qaW8Woc
qJ9oNEPlrzqXzRM27rqweGqpfNUQKq8ih+G2YNZR57olgGjvc5cGzL7tDixY1esl
c8Q5jg+nAkEAxzYUMdLfjZKOW+uj6CyMnoAdu+B51a5dzFwGGynh82ThAvgMRTBu
WTB0ojXdACwoPeoNBpQL2dm46T66TY4hgwJAShxpPu3R5UjyLgWsrHktl+4UIBIN
7YopZYve4n6lJGCclP2mhee4+EVkMe1v2117TVhAH7JSgl1V14vgBWNqzwJAGbHC
9w4w4WzG10RcdsTQOI1h+GqirEn6NTKIYvmK+D7Juv1Nb9soUH6nlcqGv8/yPNlk
bfXIdYfctEVbI1piwJBAJQipFo6DrVHr66iHMUecadbJ5iSX6Z7L93tjFeV2q4i
tr493M+tOzVLa7tnS6QBK53rDOCNetvbAIE69IBIgNA= -----END RSA PRIVATE KEY----- Certificate:
/etc/ssl/32015/ca.crt subject=C = CN, ST = BeiJing, L = BeiJing, O = iKuai, OU = iKuai, CN = download.ikuai8.com
issuer=C = CN, ST = BeiJing, L = BeiJing, O = iKuai, OU = iKuai, CN = download.ikuai8.com notBefore=Aug 29
04:13:19 2017 GMT notAfter=Dec 30 04:13:19 3016 GMT serial=BD9552A22264C655 SHA1
Fingerprint=68:7C:26:F4:B4:20:1B:C5:04:AD:31:58:0E:4F:C1:04:08:6C:39:B6 -----BEGIN CERTIFICATE-----
MIIcCrjCCAhegAwIBAgIJAL2VUqliZMZVMA0GCSqGSIb3DQEBCwUAMG8xCzAJBgNV
BAYTAKNOMRAwDgYDVQQIDAdCZWIKaW5nMRAwDgYDVQQHDAdCZWIKaW5nMQ4wDAYD
VQQKDAVpS3VhaTEOMAwGA1UECwwFaUt1YWkxHDAaBgNVBAMME2Rvd25sb2FkLmlr
dWFpOC5jb20wIENMTcwODI5MDQxMzE5WWhgPMzAxNjEyMzAwNDEzMTIwMG8xCzAJ
BgNVBAYTAKNOMRAwDgYDVQQIDAdCZWIKaW5nMRAwDgYDVQQHDAdCZWIKaW5nMQ4w
DAYDVQQKDAVpS3VhaTEOMAwGA1UECwwFaUt1YWkxHDAaBgNVBAMME2Rvd25sb2Fk
LmlrdWFpOC5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALCtDbswXNXT
T5JzjWSiWVgBPw5FpsvbnKHdXMKHpm6o1y2GE15+78Kw9SS/qsfsUOp1shwsyZY
VLhc55rlcD5AUgSOGHm0e5nXwUwrDAHgNFe/1MiuSluHWKPNL3wg1l/mqUyOUcG
ac156dX3pRNC+uG7mnRdVLaXWpG4WII1AgMBAAGjUDBOMB0GA1UdDgQWBBRi9kTg
MrvzSKw/dPRBP3OFFbAUcDAfBgNVHSMEGDAWgBRi9kTgMrvzSKw/dPRBP3OFFbAU
CDAMBgNVHRMEBTADAQH/MA0GCSqGSIb3DQEBCwUAA4GBAHSAppGkHlnMqhH10fDO
ciEQy8Vk1wxu4cdCi3JbhFyj7q86/SyBlxM3/Jw+fXxvto6E4w2Cbycy54I0ve

NYARC-014 | CRITICAL | CVSS 9.1

Embedded CA: private key + certificate leaked

Description: Private key and certificate pair found in firmware. Any attacker with the firmware can impersonate this service.
Evidence: Private Key: /etc/ssl/32016/ca.key (1024-bit RSA) -----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQC5kznn8oZ1SJHgzi073K8Hd826ztYpQ4CW2pDf0fmotKcdg10J
varwXW6HLCE8491TVW/AGX8t6+KUM0B9pZi5kv2IRIYj6fASuHrudPuv2MeCqmij
k3YrrUBV597IB8SAMJ1LltDwHpN8e40Q/VefRwLSfD0bBD5c99YIEh86NQIDAQAB
AoGAB6gba4aGJbCo1C2cZivkzNoUkvCVxX4TgCXkdFelhWBuxLj2zcAVnXU9ajZY
LWL5bsbHpZVnue1Rm+vBbW23r15k8RGIgfc97ome6ZWojlV937zc1Q/p8sH5IGQO
5Ct9mtp/VAzSoDFK/siWoE4sQxz/XXH5nY+fxTj02odfcAECQQDsztjq9iAbc0We
o5s7yz8WCNccAjIMLnt3zNUVA+Iskd8uOT2fEsYCSFby5ynfb00l5v9ALmC/APCz
o/lxVG7BAKEAyJ1t0PHZvR07uSTC4qSzmLCKuqelt99bAlZ/k002/wGOEJmMkZ6i
7EaYP2zxRBY7V8AjTAY0+vE2c9hAMucdQJAKm2NE9vxOLnYeWnawEXUEcCXud7y
1Jfnazl53AANbHREkVfLlcSjwoi+fZM3EKJ3Eac6QTMnJKYjbcNVc7KgQJANO3s
SmN06kDpl3iOfpOr2s5BW+vdejzQ2zYNJMULj5ReCgK1gk/w40AoENTCH61pxAY
qieVdVxQLJndaYNO/QJBAMLISKJW8/Nmaawi0GtZ1WkEdvKy1KIZ5/sXN1Nupmly
G1TDtdaNNHbeyNfLWI7NPNLmf0+unGlp7jgJQlrDY= -----END RSA PRIVATE KEY----- Certificate:
/etc/ssl/32016/ca.crt subject=C = CN, ST = BeiJing, L = BeiJing, O = iKuai, OU = iKuai, CN = download.ikuai8.com
issuer=C = CN, ST = BeiJing, L = BeiJing, O = iKuai, OU = iKuai, CN = download.ikuai8.com notBefore=Aug 29
02:15:37 2017 GMT notAfter=Dec 30 02:15:37 3016 GMT serial=92EDE68AEB529720 SHA1
Fingerprint=B8:4C:CB:B7:53:F6:70:9E:B8:D8:20:DB:8A:34:49:BE:85:E8:30:F0 -----BEGIN CERTIFICATE-----
MIICrjCCAhgAwIBAgIJALt5orrUpcgMA0GCSqGSIb3DQEBCwUAMG8xCzAJBgNV
BAYTAkNOMRAwDgYDVQQIDAdCZWlKaW5nMRAwDgYDVQQHDAdCZWlKaW5nMQ4wDAYD
VQQKDAVpS3VhaTEOMAwGA1UECwwFaUt1YWwkdHAAaBgNVBAMME2Rvd25sb2FKLmlr
dWVfOC5jb20wLmBcNMTcwODI5MDIxNTM3WhgPMzAxNjEyMzAwMjE1MzdaMG8xCzAJ
BgNVBAYTAkNOMRAwDgYDVQQIDAdCZWlKaW5nMRAwDgYDVQQHDAdCZWlKaW5nMQ4w
DAYDVQQKDAVpS3VhaTEOMAwGA1UECwwFaUt1YWwkdHAAaBgNVBAMME2Rvd25sb2FK
LmlrdWVfOC5jb20wLmBcNMTcwODI5MDIxNTM3WhgPMzAxNjEyMzAwMjE1MzdaMG8xCzAJ
keDMjTvcrd3zbr0i1ldgJbknR/ai0px2DXQm9qvBdbocsJ7zj3VNVb8AZfy3r
4pQzQH2lmLms/aVGVipP8BK4fO50+6/Yx4KqaOOTfKutQFXn3sgHxIAwnUuW0PAe
k3x7jRD9UR9HAtJ8PRsEPlz31iUSHzo1AgMBAAGjUDBOMB0GA1UdDgQWBbTtjca
FxrurcTwB+H56/Jb4Sr3JGjAfbG/NVHSMEGDAWgBTTjcaFxrurcTwB+H56/Jb4Sr3J
GjAMBgNVHRMERTADAQH/MA0GCSqGSIb3DQEBCwUAA4GBAHm1BFgWOnbJPpytu1jD
jZaoY1ISDQ+m1uyV6iJQZsK4z1ZbUnuEnGOuxCrZne8ImqasGfZrIG8JNgUha5aF
BZhzMxRuhFVWH+h0i+g+JU8n0TUMbZg4pOdOo1JLA8OAgAVB3xzc7zppGRmLfiT
6tQNdGHbLroSBHgyPVYa4Uu -----END CERTIFICATE-----

NYARC-015 | CRITICAL | CVSS 9.1

Embedded CA: private key + certificate leaked

Description: Private key and certificate pair found in firmware. Any attacker with the firmware can impersonate this service.
Evidence: Private Key: /etc/ssl/32017/ca.key (1024-bit RSA) -----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgQDA9hst5iObBs01uclvrAPqSaa1UK4HSGFiraQhMEoBdWxjO5sy
dkyfZQ4IE4A2mpSticvs0+C02DKd3mGFFeJ6Wkx2FOjEnr8JumrHLtXFlozZ8myw
aD51Tmarf6m9Oo6O63fRVXmYJHN0jy/SEHU03mxYcOvnK11DGZBuwD/FQIDAQAB
AoGAL2aFaLIG/xcd09v84r+r7h3lyNaH2YwjOBzvZGctXUxeEsZaqlu6+NDXMI6x
yTgR28tkx8mlgoQ1cuhk5k9qil+J2OBtpYho1cZ3TJyjr0d4We9hdmlAwfyvEgQ6
cl8wtpwSDreLxXXjV7pBAUjcxemqqvYOkW1x+1qIEOmK0ECQQDrsWmVPSu2UOLS
9sy0okyRmBPEDFLGI0u6MGgq8moJm49c7X/Ld3p/+68KToKrRgZLHi4CEjkZu
JRZi2QpxAkEA0ZYtpjELUbfTwcPZ2SUUr3E+el4YC+rAu65F4vV1vlwozzW6wH7
4Zvml0umyOPE2EhSdyBQVFQFdzVDm0ko5QJadeYOScAKsK1veVZJegZB1V/M55PZ
HMpov+PunfQdn3XvBk8sqB/L7l5hrHQkphJVwG1Pjg/jXuuloapds16ckQJALwoK
wtMdHD+7R5LicQcOhnXfNIWHxhzxFu59M122J+KiMjD0d5hhZPhtiE3taGgF19lb
kNsSzGpzM5cjzlv0NQJAMQ/92b9AHQA7dXoFKS3KRpWBtzvGtDoYg7Zvz5usHR12
96gWDLiY8BLsIOESohKzyFOd5qNhrVUBENvIKOelBA== -----END RSA PRIVATE KEY----- Certificate:
/etc/ssl/32017/ca.crt subject=C = CN, ST = BeiJing, L = BeiJing, O = iKuai, OU = iKuai, CN = 302.ikuai8.com
issuer=C = CN, ST = BeiJing, L = BeiJing, O = iKuai, OU = iKuai, CN = 302.ikuai8.com notBefore=Sep 6 04:04:56
2017 GMT notAfter=Jan 7 04:04:56 3017 GMT serial=E43325EF748B108B SHA1
Fingerprint=EC:29:58:77:4B:E1:99:CC:DA:74:14:A2:B9:0B:D9:D7:EF:C9:D5:36 -----BEGIN CERTIFICATE-----
MIICpDCCAg2gAwIBAgIJAOQzJe90ixCLMA0GCSqGSIb3DQEBCwUAMG8xCzAJBgNV
BAYTAkNOMRAwDgYDVQQIDAdCZWlKaW5nMRAwDgYDVQQHDAdCZWlKaW5nMQ4wDAYD
VQQKDAVpS3VhaTEOMAwGA1UECwwFaUt1YWwkdHAAaBgNVBAMMDjMwMi5pa3VhaTgu

NYARC-017 | CRITICAL | CVSS 7.5

OpenSSL 1.0.0 - End of Life

Description: OpenSSL 1.0.x reached EOL in 2020. Contains numerous known CVEs including potential RCE
Evidence: /usr/lib/libssl.so.1.0.0

NYARC-018 | HIGH | CVSS 5.3

Generic backdoor detected (CVE-2023-50920): Lua random seed (check for predictable values)

Description: Lua random seed (check for predictable values)
Evidence: /usr/sbin/ikntpgt
Solution: Update firmware. Use /dev/urandom for session ID generation instead of math.random.
CVE: [CVE-2023-50920](#)

NYARC-019 | HIGH | CVSS 5.3

Generic backdoor detected: JSON parser library (sscanf overflow CVE in parse_object)

Description: JSON parser library (sscanf overflow CVE in parse_object)
Evidence: /usr/sbin/miniupnpd
Solution: Update firmware to latest version. Review vendor security advisories.

NYARC-020 | HIGH | CVSS 5.3

Generic backdoor detected: JSON parser library (sscanf overflow CVE in parse_object)

Description: JSON parser library (sscanf overflow CVE in parse_object)
Evidence: /usr/sbin/pmd
Solution: Update firmware to latest version. Review vendor security advisories.

NYARC-021 | HIGH | CVSS 5.3

Generic backdoor detected: JSON parser library (sscanf overflow CVE in parse_object)

Description: JSON parser library (sscanf overflow CVE in parse_object)
Evidence: /usr/sbin/tkgen
Solution: Update firmware to latest version. Review vendor security advisories.

NYARC-022 | HIGH | CVSS 5.3

Generic backdoor detected (CVE-2023-50920): Lua random seed (check for predictable values)

Description: Lua random seed (check for predictable values)
Evidence: /usr/ikuai/script/ik_netoptimize.lua
Solution: Update firmware. Use /dev/urandom for session ID generation instead of math.random.
CVE: [CVE-2023-50920](#)

NYARC-023 | HIGH | CVSS 5.3

Generic backdoor detected: JSON parser library (sscanf overflow CVE in parse_object)

Description: JSON parser library (sscanf overflow CVE in parse_object)
Evidence: /usr/lib/libjansson.so
Solution: Update firmware to latest version. Review vendor security advisories.

NYARC-024 | HIGH | CVSS 5.3

Generic backdoor detected: JSON parser library (sscanf overflow CVE in parse_object)

Description: JSON parser library (sscanf overflow CVE in parse_object)
Evidence: /usr/lib/libjansson.so.4
Solution: Update firmware to latest version. Review vendor security advisories.

NYARC-025 | HIGH | CVSS 5.3

Generic backdoor detected: JSON parser library (sscanf overflow CVE in parse_object)

Description: JSON parser library (sscanf overflow CVE in parse_object)
Evidence: /usr/lib/libjansson.so.4.13.0
Solution: [Update firmware to latest version. Review vendor security advisories.](#)

NYARC-026 | HIGH | CVSS 5.3

Generic backdoor detected: JSON parser library (sscanf overflow CVE in parse_object)

Description: JSON parser library (sscanf overflow CVE in parse_object)
Evidence: /usr/sbin/cre
Solution: [Update firmware to latest version. Review vendor security advisories.](#)

NYARC-027 | HIGH | CVSS 5.3

Generic backdoor detected: JSON parser library (sscanf overflow CVE in parse_object)

Description: JSON parser library (sscanf overflow CVE in parse_object)
Evidence: /usr/sbin/ik_rc_client
Solution: [Update firmware to latest version. Review vendor security advisories.](#)

NYARC-028 | HIGH | CVSS 7.5

Remote control configuration exposed

Description: Cloud control server endpoints visible in firmware
Evidence:

```
etc/remote2/ikuai.conf { "as_server":{ "host":["as-v4.ikuai8.com:9444"],  
"ca_path":"/etc/remote2/ca-certificates.d/ikuai" } }
```

NYARC-029 | HIGH | CVSS 5.3

Generic backdoor detected: JSON parser library (sscanf overflow CVE in parse_object)

Description: JSON parser library (sscanf overflow CVE in parse_object)
Evidence: /usr/sbin/ik_stats_collect
Solution: [Update firmware to latest version. Review vendor security advisories.](#)

NYARC-030 | MEDIUM | CVSS 5.3

User 'sshd' uses MD5crypt weak hash

Description: MD5crypt (\$1\$) is a weak algorithm, recommend migration to SHA-512 (\$6\$)
Evidence: /etc/shadow: sshd:\$1\$BKY7uz3G\$vw5dPaPb...

NYARC-031 | MEDIUM | CVSS 5.3

User 'root' uses MD5crypt weak hash

Description: MD5crypt (\$1\$) is a weak algorithm, recommend migration to SHA-512 (\$6\$)
Evidence: /etc/shadow: root:\$1\$9.EU8ltY\$z4EfK4vQ...

NYARC-032 | MEDIUM | CVSS 5.3

Generic potential vulnerability: Telnet on non-standard port (potential backdoor)

Description: Telnet on non-standard port (potential backdoor)
Evidence: /sbin/sysinit
Solution: [Review this component for proper input validation and access control.](#)