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 23:24:54 UTC
Tool	Nyarc Professional v1.2.0

RISK SCORE: 56/100 (MEDIUM)

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

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/A5nDgSA2zLX4rX8iSIV2KwmCgr2Ov8h3hDl+FFsdYu63/Lhf74YS50LJ/4
b0jaljIXLZ3tg1usicnorTxZEz+i7C6/qOYsch7KTVNk1JTQ6hwlmrZhyNIs4vgi
tKT8rLnPzkw5qLm0nbdjPHXeGt8SxH/yeFaKWpQo6vwH2+DD6YHJ/haprRd2Mqr5
3mRnfHe1TodaWdO+td6VBd3RND3kVCyF/uUBwhlH9lXRq4benqHIJATq4U/QymMC
AosHXFi389K45/Ck8XMxcz84+ESmjZLyVEsS66D1GyyVqoe0B6y4e+aQnE28cFMZ
+oHPWRfbFHGtWeRw/n0fo8DVx5BSrfcO3I2/WIDLSMbK+s5EkN8Q974nDhqZQMP4
tc0efp4qNjhTichkSpaIErS0Ws1hEnILMUXR+3bsjgl9E+4nfE9dEad79L9evkds
/ywPC32x6FWVjGXty1lT5gUVw4U++WKf2oj7lUh+39qEXzjOd2IRMZeRo/21EWR2
ep1Fp7fm2jRF74fliB91Muqh2AEhG0dgOPQucvnyh/wahKRwdTUBxtnN2EKhN4qx
FO79S2s0B6+rDuLvjt3+tg5bPPIMe1/n8l78qnLwnH93f9WxWsRwxnE4MwOeP+Fj
aozRwxX6jOapEhpMSkOJ0rNCi+bH+bupDbm17WWddeseqkJxeFpIGEcJ5BfzVZER
n20GAtELoAA6jg9JR8piVQw2LC/RB6zaOO/GCid6My1tYnn5deXpRIKCEru+mH58
9oQ2oMxy3akJ3nFo/fBpTGyMkqye6jhrUQ9XYTNU3IubavGmpFwVZQ== -----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: sha256WithRSAEncryption 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
CQYDVQQLDAJpazEVMBMGA1UEAwwMKi5pa3VhaTguY29tMB4XDTE5MDgyMjA5NTIy
OVoXDTI5MDgxOTA5NTIyOVowWTELMAkGA1UEBhMCQ04xEDAOBgNVBAgMB2JlaWpp
bmcxDjAMBgNVBAoMBWlrdWFpMREwDwYDVQQLDAhpa2NsaWVudDEVMBMGA1UEAwwM
Ki5pa3VhaTguY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDukENI2j53
ECNNVLmVR0sAMXRRe1WdDPKYLgDjHFYD/FaX1SNc9RIyQk+w3iQccxDXocptNCPx
EPetNKIfPbd2mkoDUczlW+nuwtIOIxFMtv/LQY8dhaxdWM4HJM7ejyKvE35eEKVM
4AvVA6SdeeW74l4ee0Pa0eXACg7PtVqiFwIDAQABo4HXMIHUMAkGA1UdEwQCMAAw
LAYJYIZIAYb4QgENBB8WHU9wZW5TU0wgR2VuZXJhdGVkIENlcnRpZmljYXRlMB0G
A1UdDgQWBBRxmpYaEZIdg/fC7hcc0d7futmPkjB6BgNVHSMEczBxoWSkYjBgMQsw
CQYDVQQGEwJDTjEQMA4GA1UECAwHYmVpamluZzELMAkGA1UEBwwCYmoxDjAMBgNV
BAoMBWlrdWFpMQswCQYDVQQLDAJpazEVMBMGA1UEAwwMKi5pa3VhaTguY29tggkA
+70JCd5DCJswDQYJKoZIhvcNAQELBQADggEBADisuf0ftWUIyTrYad/js1ZGHEdL
jgcJEleq2jRn3TLP90W3o143EcLtJvapucisUuXC4DgcJYEs2oE45NQnw3yQ3LE5
ivdZugsb9nYHtFwBnGjTUlEI2T31HAh9ZB9thQ46HHM1jVKNwZ2tknUvXBManEIW
jlJTNmyfr57cVjcJpkMctzDQNGW5pKBs5rV+l0OfAJIBWNnnfTMwPsB/jmZy2FwR
ttUOOSTTT3nVN7L4E3Xq8SBmNMvn6xLM4DU++8nox4ZdM51V0fAaiSyTum/kefv4
NTpBqPiUf1Wlvw0nBF4x+nRyz6+MPwjl+e3Dy/6o92eDCo9DzSK7fbwNt8I= -----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-----
MIIJKAIBAAKCAgEA9QQ1rQPfVl5bMoOYdZqzNz1Sb77M0agE+VSm63KlC1J73MSc
VJZ+2tQE8ro8zgShhvvIUggZcKTqqZeNjUA9N/6yBVQdOBRh/Bj4FIzY8lOvYt1z
a35gGZW7EsMfmhsQ0JKEih1i2JW0riWvh6h60dIKslPbd6DIebz3ViNWtljUC13t
NqTiFb3gMyNcI72354fFbcWRKANNk7EFVuz35DRqaRRDtjY/KOskyYBSCZO1/tE5
vlwFeQgUBZBL9kswoTNS7esHdg9OolLRezt44IpHe7xqpH23/Yc0d/oYS4CsCHY1
LkE/Z69fjYTvo2+SKDTSit9chcRWPifznZetY5MnIcd93qS5mGCfjx4AcyvmXoQx
KfN1A9pnm2XWxWs0MMLK1xIyvjxn3pbSpF/Cj7WUx3NBAuCIK7PvRt7d+tu+6MuY
S4UdzGwL1isseOYQ4y00jSiQLmus/y1iFiQ/nf+MRZd+yK4adDcj6fQsXRNrbtLX
dG2friGi99TOft914zVH733ZRvvf+0OOecynU198bvGh23ecNp/CMymYCKhi+Joi
h7/7Bdm+mZ7GUwbPJ63MJJhqbKppwNBVDblAzejOmwHLtvSPxkpu49MmtRADMu8U
BfDvZspV44ciIeZtV/w41votiIpE9puJsde7HcNuouz2v9WHxyM6J2H1+IUCAwEA
AQKCAgEA1xAT4ULV5aS63fL+frQEfQc5ddZ/R8P4YbX5Mg+WaQLEr/pv0hurS37w
vPHV72vHMImOwtpTIjnPtH7Pg92QHrdUITM81n2lqDdugfNDdikYeGozJnZt+ecg
po5ZDdaWAs2owuaaXcvCJV303dl3vPZl5zOOH0okzh6c56HrOfFsZnHShrVhsX3R
7nEqLkEXzIWzOPBCwmFr1ah7LFqiGFAd2xArgyPIeq0zxB77Y2ahSAL0cW+qahs6
H8wRsSU8kTJQp382NF2pQvf44fdI2abmqeivnqSvPD1SQ8FlU9ikqGTBt1EUS3l3
IOw/wDBtlRcQe08lklDM9o/w2TJKwLWrLFdVoFkhMHSmzz2hMQooRupsqo6nm7yG
JGYXXteVfpJaw+nUpHUPWM9+7ax/kojv6ioVLoEn8ZhSD3eo+EzsXb7UWXCQwiqi
VZYwaOH0/6jnrDg1hbOZbGwiBBx9fpIf18PwZ+mMXTHdhhagMIMzRB+UxvJ1aqzt
AgJRq+9PlvqE5/QofS7WJjPMkCyFlCva0WGxsWcE004gwN2TJ4owsSSLq2MB10uM
omWHUur0Br+2VN1i1+9maHy6m534aOO9damPTgkku3XMHJAI+YTzvvymAJm3l+uX
e5Byj7zKRv7tZ9Knkrwb5bMp5pTDiGnYmwSIPUAi6VwmvIgjp8ECggEBAP8I88tw
3/AHykpGnCtopNob8M/Ypy22HOsymtsg79MFc28ysl2TIBk69bIH2IF2TkwE9/VZ
aRP/YHGuxxMy1rgFQuVI4OIFIID/y0dA4PzpOBQ3Yhjn2ZWekro3zjV2aZ6T38Mk
2GJkH034JdUCOR7d5RQ4pGZp+z/BGhkR+1oGUaOwZMXEJjlVXniOYYvhXhDWagma
iXMJIo6QAlHIuJPk/fzAoH5BXOjTgUg0ClxQJmNZ+pe5jLIeGwbK31YkH++4FT1N
5uzqd+ADS/z6hL/WvFaKd6xgxpIGzRqQu6vjo4j+dviJZNljmNZyQAqBjDCpIf08

1FvjVBUyzg+rZFUCggEBAPXxjXZSO7FoawDg2dQaPCnG+GpRYI69cfNMHxd47b3d
nrI7SbcuD0gXTe2eP6uqmbYzp44tfBZxIhc3GMc6zKzOsLQ2pTPe5A5hNK4gNVBn
zW1cCtQfltv/Md+TUsaWtRzQJDLGlmNFQ/6T7tx1cBjeKV70OmfXM6hLDD7sBNhi
zLLU0KrqsGBoYrDdexw5fOCbhR6zDyLyRsX9v8vsUssMfMvrXxytDRHZtU5oDtjm
JSXFa8huqtCusVAR8Et7LBC+b+mOwah16bxPoE8oq6pMeoKjQ38CmceWSCWc4Cws
JyUsam247LyBiSMfWWuYU6jwJFphKSiDiIN5eyzK83ECggEABZKUgSV+PyhsayMP
1oL61yk1IdWCEaWhDCKW76LQmrPLyeo5q4HDecmoBLPXLzz+iPqy0FGb0iwKV3GS
OAEsX+j9hTUKdOXXx/nO30ezotMVvptXMWQfhP1qB1eg0do8hJKGmST89WlqpbF+
YiEiTmJa1w5FyVcXflUh1Npnu5fXwNPh39BhZW9QGSJDT2MlQwjsWDlgN3tDngnX
gyH3poOiaRtsZlXXSd8VPBanA01dCV618wrC4EF4JbXZG3C+oeZL0IMbQKH+7I4l
4uk2bVqr0thDtSiILjin0qTG9QKMWDn3L4cRBQ8AD+9/Jrud7JJFg9sIaNmWxL/P
cNg14QKCAQAkbn+yA0RsZzdSjfw2exxmY97wgNV4z39Ntvz0ESnGcknLxRSKWfxR
hYI5rLNpzn+uicBMQ1iaSm/uWG8HNCKVhpiOWXnnUSEfMC8JjCPZoUbA6F2CRpum
Qws0PzKH0FNLzVIPXDNyyRPlZix/47WTOXWPZ0Yvk6VHTLanq3acRyZjZzrx1ooB
/fSAlo5iA/IHo4H4pjWby5/IPGpo3rz07widfGQ+bzP8bO96ideJMa5XBgONUTdk
ajxBzCZ4R+qjIFKbmlX9ilnxVyo8D54+P832BBE/gzccZZqSV8atRG0YCJhLYJVQ
5y9VUJOCaLIb2FbKPJJIOhPCxgAFBptBAoIBAGHueyuSB//B+00dZJL77SM5AloX
pdgJzDw8bAYDpac7X2PvdqI/GsrqxYJGbAoShcPtHhAWKSYK8bZXKME2tTHFvlJR
qF5lWMt0hoKx85CT9LMLUnPLT1ockqvNlqf0UXolVsWKJQm6W9na4G46h20vTCRy
zvCjOxciH4NxFARwsqjjmk4JAEQ8Vv0UC0ErHkW0jkOr3r4SpcxtvDEV+r+nFbeh
5w/MStqx238k+pyQ/A7MlZgzsWjFCd+krmKIceUalUgQ874zVsGGrAoAz6mEf+f2
V991EHS0XAVhtHIKFqG///seYEVxGdBtOdGeXQhaTpn7TjuYH+2c8/Igf2g= -----END RSA PRIVATE KEY-----
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 -----BEGIN CERTIFICATE-----
MIIGezCCBGOgAwIBAgIDEAAAMA0GCSqGSIb3DQEBBQUAMIGwMQswCQYDVQQGEwJD
TjEQMA4GA1UECAwHQkVJSklORzETMBEGA1UECgwKSUtVQUk4IEx0ZDErMCkGA1UE
CwwiUkVNT1RFIENPTlRST0wgMDAwMi0wMSBGT1IgUk9VVEVSUzEsMCoGA1UEAwwj
cmVtb3RlX2NvbnRyb2wucnQwMDAyLTAxLmlrdWFpOC5jb20xHzAdBgkqhkiG9w0B
CQEWEGFkbWluQGlrdWFpOC5jb20wHhcNMTUxMjI0MDI0NDIzWhcNMjExMjIyMDI0
NDIzWjCB0TELMAkGA1UEBhMCQ04xEDAOBgNVBAgMB0JFSUpJTkcxEzARBgNVBAoM
CklLVUFJOCBMdGQxRjBEBgNVBAsMPUNFUlQgMDAwMSBPRiBDQSBSRU1PVEUgQ09O
VFJPTCAwMDAyLTAxLTAwMDEgRk9SIElLVUFJIFJPVVRFUlMxMjAwBgNVBAMMKWNl
cnQwMDAxLnJtX3JvdXRlcjAwMDItMDEtMDAwMS5pa3VhaTguY29tMR8wHQYJKoZI
hvcNAQkBFhBhZG1pbkBpa3VhaTguY29tMIICIjANBgkqhkiG9w0BAQEFAAOCAg8A
MIICCgKCAgEA9QQ1rQPfVl5bMoOYdZqzNz1Sb77M0agE+VSm63KIC1J73MScVJZ+
2tQE8ro8zgShhvvIUggZcKTqqZeNjUA9N/6yBVQdOBRh/Bj4FIzY8lOvYt1za35g
GZW7EsMfmhsQ0JKEih1i2JW0riWvh6h60dIKslPbd6DIebz3ViNWtljUC13tNqTi
Fb3gMyNcI72354fFbcWRKANNk7EFVuz35DRqaRRDtjY/KOskyYBSCZO1/tE5vlwF
eQgUBZBL9kswoTNS7esHdg9OolLRezt44IpHe7xqpH23/Yc0d/oYS4CsCHY1LkE/
Z69fjYTvo2+SKDTSit9chcRWPifznZetY5MnIcd93qS5mGCfjx4AcyvmXoQxKfN1
A9pnm2XWxWs0MMLK1xIyvjxn3pbSpF/Cj7WUx3NBAuCIK7PvRt7d+tu+6MuYS4Ud
zGwL1isseOYQ4y00jSiQLmus/y1iFiQ/nf+MRZd+yK4adDcj6fQsXRNrbtLXdG2f
riGi99TOft914zVH733ZRvvf+0OOecynU198bvGh23ecNp/CMymYCKhi+Joih7/7
Bdm+mZ7GUwbPJ63MJJhqbKppwNBVDblAzejOmwHLtvSPxkpu49MmtRADMu8UBfDv
ZspV44ciIeZtV/w41votiIpE9puJsde7HcNuouz2v9WHxyM6J2H1+IUCAwEAAaN7
MHkwCQYDVR0TBAIwADAsBglghkgBhvhCAQ0EHxYdT3BlblNTTCBHZW5lcmF0ZWQg
Q2VydGlmaWNhdGUwHQYDVR0OBBYEFNFRjG2/Q8K6In5EqF4El7N+aF0BMB8GA1Ud
IwQYMBaAFMyp0r9lX2v0B6BWtmVw85u6SQ/BMA0GCSqGSIb3DQEBBQUAA4ICAQA4
iOWLpnXqN7t99mb10D/3L7DDLB1y3a9J5OptO7wxb7L+Hr8YawSsdf/pkmD4AEB0
/SMJ4k1/qeZa2D/n57Tn6tHu7xqdhjSo4an0jmDvv6wQkwPi4zTlK5yxk6XJtN1R
ECXOMFrlvj6CkWU8bkAiux8thGNHTkRwtteRiindgXkJPAtg68ULdriZKQhcJm19
o97/btaI6szY6iHL1rmfEV08gV3H7EwVztPCsrD5Temhk+2EIkqsT0u1Rqvqs5so
j6+CBAoaXXuVWTMK9CbwQnWJooswHiSPefBPZ4HujO7HvUpIFnubA5FSTk60ICVO
sZI51i3LNewmgfEjLifGZAcNQF0mcxeDMJXI7To49atqiqqDAQfJ5dYooJlaE3oA
vfF0USv8KvRmz4+v/8EQFEIDEm/k7l/0NRlPNFNP+p+spQ0SxhbQTTsNVPRWioMk
65z2nnSwctUjH34t6rOvh78herlJ1+fxOsJlpM57CGt7ojVvpLbwVSh03Fz8Co7z
DRcDmG8i/XcD1Tz0G4UXiAqQ2eyCew9TppPkAaVywoz1a/chRRmwpxpE8oaQUEqF
viUa5k+86SlINZAyw40/VNOCeFNYCDxFzQ2jxB4h9YyZgGHKsc5/DRkbZ8tQeTQ3
K6DxRBmMv80Z+UT8T+aIpkcjf7hcplDYFtejTTpdog== -----END CERTIFICATE----- -----BEGIN CERTIFICATE-----
MIIGKTCCBBGgAwIBAgIDEAAAMA0GCSqGSIb3DQEBBQUAMIGqMQswCQYDVQQGEwJD
TjEQMA4GA1UECAwHQkVJSklORzEQMA4GA1UEBwwHQkVJSklORzETMBEGA1UECgwK
SUtVQUk4IEx0ZDEhMB8GA1UECwwYUk9PVCBDQSAwMDAyIEZPUiBST1VURVJTMR4w

HAYDVQQDDBVydDAwMDIucGtpLmlrdWFpOC5jb20xHzAdBgkqhkiG9w0BCQEWEGFk
bWluQGlrdWFpOC5jb20wHhcNMTUxMjI0MDIzMTMyWhcNMjUxMjIxMDIzMTMyWjCB
sDELMAkGA1UEBhMCQ04xEDAOBgNVBAgMB0JFSUpJTkcxEzARBgNVBAoMCklLVUFJ
OCBMdGQxKzApBgNVBAsMIlJFTU9URSBDT05UUk9MIDAwMDItMDEgRk9SIFJPVVRF
UlMxLDAqBgNVBAMMI3JlbW90ZV9jb250cm9sLnJ0MDAwMi0wMS5pa3VhaTguY29t
MR8wHQYJKoZIhvcNAQkBFhBhZG1pbkBpa3VhaTguY29tMIICIjANBgkqhkiG9w0B
AQEFAAOCAg8AMIICCgKCAgEAwYBgUKTWOwz0j+sE6xC3HBiADjRH8a4Gq/fcuGML
+I2SqbeDOAT95PFwCptDkFVx7Aqs6NVirVm80XOFp23R+ZCzXYtcNFcZ1JsfIEgB
oZPyEjoCKu7kVoRC0yti+3Ay4sRh4+I702LZWDYQHFvKC3bRiHKs8rUlPiSST4It
r0WHnKXBMxDX+jOqMd0vhqf2iYHZ9KRs4BNSbdW+pEFdGmluC5UIBoZGikWC8+x/
WpB6uPR3rp3xEcPdUYeF1xe64TFZDg62cdvxAMXSEvSJ6XWYN37CQnUBzDRY4jpO
db1SoZQ041QTlVZ2Ng1U0pjEcciOnxznYyluT3hkkdMS1tkLHqY7YrFlYhSKxy7u
Yapm5b5m9FG8b9P8TRZbwK9P1gby//OLufz1CZ9TZh1Gao4ha1CkHKL7r9Bqm8FU
pmLOGAbmCLnlDcD61iVJFkomU1fHl5Cpv4Cgzhiq7nqngAcG4uxshLAsKvTEnLtr
mQ8yhkD5TZxTxGYjDM7ruff8fURSxoPu7QMdfFnLFhwizMTf7RwsHjvGVX0xDjhG
X+41/Fwb9UmFZXUBx9LU4kEEiToM0Oj/tfz1KN3Y4uTtaogVdYoBeQEtzynaRFJk
2nj4oYL7bhJEI4PKwEzWILNKXcqxkOfDNE+F1jBPUN3VyCEm3EhYkCZUHTKnFGQJ
UUsCAwEAAaNQME4wHQYDVR0OBBYEFMyp0r9lX2v0B6BWtmVw85u6SQ/BMB8GA1Ud
IwQYMBaAFDhs+J6vp0PnP57q4/Gk6iqjAn0UMAwGA1UdEwQFMAMBAf8wDQYJKoZI
hvcNAQEFBQADggIBAEmNEDAwQl0coYE0JmjgZGwSnes0Gi2BPRMR4/2ZPA5MBQ55
C3Otk+Clrw/zcUz4TX87q1Mx0wn263VrV9Dq6qkric3OV7430LGgva0GW3lS7/3N
zo3t9jMw/OULM+IgsW6ADjHWv4c0JGJ+f+fzViqKagOl7uVWEXpQ1mHZlYNo3rrs
mE+jG2T448QeNXYJE4R6KQ2CxDO9VzzD83eAJktZetZt4B+3JDtp/2zwq1bPsxVZ
3gO7N+JYSqL2DF28Y/4xSrbS9Kp9fFUeX/lpT//iMkCMjrLppU9CxCS9cTJ+s6v8
Y1CZDuaPQYqeX5InDhkmslCV6vITzLi3Odtu0ewLqpaw23ew7I9NrOkVy77zR2PP
PFU8xh5S7S+sHxYuW4/oBjLK7O8hvH0edHD/NVIZpL9FfsP1DbH9VnPL6fg8iitr
p0cMRfby2r+pFweJHnCRpU7e+I5dT264rFgxLZ9SHP2jJ3QDfIgiE+Ccjpp+zlB2
5Wz5hsZf/yE0O3AEreN+VBOOKcTcyFnEqbrBCg4sUofxTRpurJ17GNLhOASJH+fc
Jc12dfOzWKIz0sKFjMNi+g0NFTo5BW5UaFC0MXd0qRZmyP4eq/AZu9V3cTsUQxdx
ALPPSRRAhSfDHmx7sHiTHlJjjqytkVsm6bJDJoT/MRdlttV+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-----
MIICXAIBAAKBgQCwkw28LFzV00+SWY1kpVrxmz1uRT7L5wZyh3VzJB6ZuqNcthhN
efu/CsPUkv6rH0lDqdbIcLMmWFS4XOea5XA+QFIEjhh5tHuZ18FLsKwwB4DRXv9T
Irkpbh1ijzS98INSP5qlMjlHBmnNeenV96UTQvrhu5p0XVS2l1qRuFiJdQIDAQAB
AoGAHid+2PvafsmvdRbGBsIWXdxdCU/aAYhamYR4kklA0JAHBfYzAEgsrdtwxgS0
aRTWti9y9pgIgCvli/aRtuon2LDt0iAJMn8LkvmjPyLyvET4zOsZ8/IiqOILyv8E
cjpVBnjexxsWZhCiTi0AkUBNaKKrjeywxuChgCW6JlOTOqECQQDi6P+Y8qaW8Woc
qJ9oNEPlrzqXzRM27rqweGqpfNUQKq8ih+G2YNZR57olgGjvc5cGzL7tDIxY1esI
c8QSjg+nAkEAxzYUMdLfjZKOw+uj6CyMnoAdu+B51a5dzFwGGynh82ThAvgMRTBu
WTBOojXdACwoPeoNBpQL2dm46T66TY4hgwJAShxppu3R5UjyLGwSrHktl+4UiBIN
7YopZYve4n6IJGCclP2mhee4+EVkMe1v2I17TVhAH7JSgI1V14vgBWNqzwJAGbHC
9w4w4WzG10RcdsTQOl1h+GqirEn6NTKlYvmK+D7Juv1Nb9soUH6nlcqGv8/yPNIk
bfXIdYfcjtEVbI1piwJBAJQipFo6DrVHr66iHMUecadbJ5iSX6Z7L93tjFeV2q4i
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-----
MIICrjCCAhegAwIBAgIJAL2VUqIiZMZVMA0GCSqGSIb3DQEBCwUAMG8xCzAJBgNV
BAYTAkNOMRAwDgYDVQQIDAdCZWlKaW5nMRAwDgYDVQQHDAdCZWlKaW5nMQ4wDAYD
VQQKDAVpS3VhaTEOMAwGA1UECwwFaUt1YWkxHDAaBgNVBAMME2Rvd25sb2FkLmlr
dWFpOC5jb20wIBcNMTcwODI5MDQxMzE5WhgPMzAxNjEyMzAwNDEzMTlaMG8xCzAJ
BgNVBAYTAkNOMRAwDgYDVQQIDAdCZWlKaW5nMRAwDgYDVQQHDAdCZWlKaW5nMQ4w
DAYDVQQKDAVpS3VhaTEOMAwGA1UECwwFaUt1YWkxHDAaBgNVBAMME2Rvd25sb2Fk
LmlrdWFpOC5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALCTDbwsXNXT
T5JZjWSlWvGbPW5FPsvnBnKHdXMkHpm6o1y2GE15+78Kw9SS/qsfSUOp1shwsyZY
VLhc55rlcD5AUgSOGHm0e5nXwUuwrDAHgNFe/1MiuSluHWKPNL3wg1I/mqUyOUcG
ac156dX3pRNC+uG7mnRdVLaXWpG4WIl1AgMBAAGjUDBOMB0GA1UdDgQWBBRl9kTg
MrvzSKw/dPRBP3OFFbAUCDAfBgNVHSMEGDAWgBRl9kTgMrvzSKw/dPRBP3OFFbAU
CDAMBgNVHRMEBTADAQH/MA0GCSqGSIb3DQEBCwUAA4GBAHSAppGkHlnMqhH10fdO
ciEQy8Vk1wxu4cdCi3JbhFyjq7q86/SyBlnxM3/Jw+fXxvto6E4w2Cbycy54l0Ve

S/paM0LVemKegMNM+mFItxHOPbfwG3Gx0jVK+tc0dSVHxbLRZQFrLqmlLwIAQ3oO
6PTuxoiPa/b9vL+S+ugVvxkQ -----END CERTIFICATE-----

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+KUM0B9pZi5kv2IRlYj6fASuHzudPuv2MeCqmjj
k3yrrUBV597IB8SAMJ1LltDwHpN8e40Q/VEfRwLSfD0bBD5c99YlEh86NQIDAQAB
AoGAB6gba4aGJbCo1C2cZivkzNoUkvCVxX4TgCXkdFelhWBuxLj2zcAVnXU9ajZY
LWL5bsbHpZVnue1Rm+vBbW23r15k8RGlGfc97ome6ZWojlV937zc1Q/p8sH5IGQO
5Ct9mtp/VAzSoDFK/slWoE4sQxz/XXH5nY+fXtj02odfcAECQQDsztjq9iAbc0We
o5s7yz8WCNccAjIMLnt3zNUVA+lskd8uOT2fEsYCSFby5ynfbO0l5v9ALmC/APCz
o/lxVG7BAkEAyJ1t0PHZvRO7uSTC4qSzmLCKuqelt99bAlZ/k002/wGOEJMmkZ6i
7EaYP2zxRBYP7V8AjTAY0+vE2c9hAMucdQJAKm2NE9vxOLnYeWnawEXUEcCXud7y
1JfnazI53AANbHReRkvfLIcSjwoi+fZM3EkJ3Eac6QTmNJKYjbcNVC7KgQJANO3s
SmN06kDpl3iOfpOr2s5BW+vdejzQ2zYNJMULjI5ReCgK1gK/w40AoENTCH61pxAY
qieVdVxQLJNdaYNO/QJBAMLlSKJW8/Nmaawi0GtZ1WkEDvKy1KIZ5/sXN1NupmlY
G1TDtdaNNHbeyNfLWI7NPnLMf0+unGlqp7jgJQlrtDY= -----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-----
MIICrjCCAhegAwIBAgIJAJLt5orrUpcgMA0GCSqGSIb3DQEBCwUAMG8xCzAJBgNV
BAYTAkNOMRAwDgYDVQQIDAdCZWlKaW5nMRAwDgYDVQQHDAdCZWlKaW5nMQ4wDAYD
VQQKDAVpS3VhaTEOMAwGA1UECwwFaUt1YWkxHDAaBgNVBAMME2Rvd25sb2FkLmlr
dWFpOC5jb20wIBcNMTcwODI5MDIxNTM3WhgPMzAxNjEyMzAwMjE1MzdaMG8xCzAJ
BgNVBAYTAkNOMRAwDgYDVQQIDAdCZWlKaW5nMRAwDgYDVQQHDAdCZWlKaW5nMQ4w
DAYDVQQKDAVpS3VhaTEOMAwGA1UECwwFaUt1YWkxHDAaBgNVBAMME2Rvd25sb2Fk
LmlrdWFpOC5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALmTOefyhnVI
keDMjTvcrwd3zbrO1ilDgJbakN/R+ai0px2DXQm9qvBdbocsJ7zj3VNVb8AZfy3r
4pQzQH2lmLmS/aVGViPp8BK4fO50+6/Yx4KqaOOTfKutQFXn3sgHxIAwnUuW0PAe
k3x7jRD9UR9HAtJ8PRsEPlz31iUSHzo1AgMBAAGjUDBOMB0GA1UdDgQWBBTTjcja
FxurcTwB+H56/Jb4Sr3JGjAfBgNVHSMEGDAWgBTTjcjaFxurcTwB+H56/Jb4Sr3J
GjAMBgNVHRMEBTADAQH/MA0GCSqGSIb3DQEBCwUAA4GBAHm1BFgWOnbJPyvtu1jD
jZaoY1ISDQ+m1uyV6iJQZsK4z1ZbUnuEnGOuxCrZne8ImqasGfZRiG8JNgUhA5aF
BZhzMxRuhFVWH+h0i+g+JU8n0TUMbZg4pOdOo1JLA8OAgAVB3xzrCz7ppGRmLfiT
6tQNdGHbLroSBHgcyPVYa4Uu -----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-----
MIICWwIBAAKBgQDA9hst5iObBs01ucIvrpAQsaa1UK4HSGFirAQHMEoBdWxjO5sy
dkyfZQ4IE4A2mpSticvs0+C02DKd3mGFFej6WKx2FOjEnr8JumrHLtXFIozZ8myw
aD51TmaRf6m9Oo6O63fRVXmYJHNg0jy/SEHUO3mxYcOvnKI1DGZBuwD/FQIDAQAB
AoGAL2aFaLIG/xcdo9v84r+r7h3lyNaH2YwjOBzvZGCtXUxeEsZaqnu6+NDXMI6x
yTgR28tkx8mIgoQ1cuhk5k9qil+J2OBtpYho1cZ3TJyjr0d4We9hdmIAwyfvEgQ6
cI8wtpwSDreLxXXjV7pBAUjcjxemqqvYOkW1x+1qlEOmK0ECQQDrsWmVPSu2UOLS
9sy0okyyRmBPeDFLgDIOu6MGqq8moJYm49c7X/Ld3p/+68KToKrRgZLHi4CEjkZu
JRZi2QpxAkEA0ZYtpjELUbFtwcPZ2SUUr3E+eI4YC+rAu65Fi4vV1vlwozzW6wH7
4ZvmL0umypOE2EhSdyBQVFQFdzVDm0ko5QJAdeYOScAKsK1veVZJegZB1V/M55PZ
HMpov+PunfQdn3XvBk8sqB/L7l5hrHQkphJVwG1Pjg/jXuuIoapds16ckQJALwoK
wtMdHD+7R5LicQcOhnXfNIWHxhzxFu59M122J+KiMjD0d5hhZPhtiE3taGgFl9lb
kNsSzGpzM5cjzlV0NQJAMQ/92b9AHQA7dXoFKS3KRpWBtzvGtDoYg7Zvz5usHRI2
96gWDIqY8BLsIOESohKzyFOd5qNHrVUbENvIKOelBA== -----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-----
MIICpDCCAg2gAwIBAgIJAOQzJe90ixCLMA0GCSqGSIb3DQEBCwUAMGoxCzAJBgNV
BAYTAkNOMRAwDgYDVQQIDAdCZWlKaW5nMRAwDgYDVQQHDAdCZWlKaW5nMQ4wDAYD
VQQKDAVpS3VhaTEOMAwGA1UECwwFaUt1YWkxFzAVBgNVBAMMDjMwMi5pa3VhaTgu

Y29tMCAXDTE3MDkwNjA0MDQ1NloYDzMwMTcwMTA3MDQwNDU2WjBqMQswCQYDVQQG
EwJDTjEQMA4GA1UECAwHQmVpSmluZzEQMA4GA1UEBwwHQmVpSmluZzEOMAwGA1UE
CgwFaUt1YWkxDjAMBgNVBAsMBWlLdWFpMRcwFQYDVQQDDA4zMDIuaWt1YWk4LmNv
bTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAwPYbLeYjmwbNNbnCL66QELGm
tVCuB0hhYqwEBzBKAXVsYzubMnZMn2UOCBOANpqUrYnL7NPgtNgynd5hhRXo+lis
dhToxJ6/Cbpqxy7VxSKM2fJssGg+dU5mkX+pvTqOjut30VV5mCRzYNI8v0hB1Dt5
sWHDr5yiNQxmQbsA/xUCAwEAAaNQME4wHQYDVR0OBBYEFMZVUMuNDcALrA4yU9xZ
+HSH7DiMMB8GA1UdIwQYMBaAFMZVUMuNDcALrA4yU9xZ+HSH7DiMMAwGA1UdEwQF
MAMBAf8wDQYJKoZIhvcNAQELBQADgYEAnWTPob2D1Sg4blv/u0hSdQ+jU4YjI8TN
TAKdQWcK7jtfDnU20z4flu6UH99eIi1NwRnxQrf7dleBxZxc1f4dubKA6Sm1efcQ
V2/1lGc3iRspXvAJr4ja7/qf2pMVko5cePZty9YMsHgvUubRdhE2vTuYyYJYGkxY xi/KgdE4r00= -----END
CERTIFICATE-----

NYARC-016 | CRITICAL | CVSS 9.1

Web server: 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/openresty/ssl/server.key (2048-bit RSA) -----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAtvnvki3cVvbPmqHbGRDhNUl1+gYVq5nNWThZG0RHqUrVgW5a
FD3ZM8lwSxwp3xNLRqLWR5SEcXZ5IJGMSmqz5Z1BOqk9YsZcl2NkS1TiO8YidRiq
EbWWPkCO9uRsyocnQrid1BkwyGi2cUnHEl24EIzH386L1Ye24XgR82WMgXa72SmZ
HUjwN0E1YvmxdN1e4dUnsRrhDL5mxiiNTfjn5dz/H+hRZgpGrTKMXUsA6j9mofyx
wVRxPys+tLPZTKVVH0p0LDgtK5F5cWIzoFdeWVaCwqkGyMfNnlXdk+GTUpXK3oFX
FPdEuLqGCR9N3/gMDdlDxnBN2caHU4jNbVjkkQIDAQABAoIBAAKTtI8PfEnxQe1A
mFBbD4DrnvC9gzKegOjfxUmABa5ZsnYXMseUM2nqTV2RcPmGUQoWowPxEIh0jbIq
upoVtKDoPRHxbj7k4krziGcTM/h5iuSxSzvindIUoK7TesDDdIcZCIgDLs+zwdYI
nvggP8Zj5TC+vPNt7OJyCXavGHJ+Tna6nhvw9Z5wqy9LW9ZSEfxt4IMxrr3zWrP5
9uZIG2TOjR9eZfsySNRMCcWjZtiMF3X3WAytiam/l/ukVnNHm7pEwUB1/KwfRrS/
0JD1MUsfFbo+/pZQMs94Yamg1UlpHFQ37F/5jX08mVXdpGqrRs8xjHowTTjNCAnw
rbzZaMECgYEA8ceSC3OJULT7+3NAFWGf7bXiTOtrdIbUXrjPk25zZ+Ok5yPCS9T5
PsoTOVGOExOD6BYUx7iTTT31glytoupkPar+10r0ut3kRPpyifTdJIG5i6yvx0Lq
XiiA2HSUKEe6dRzW9eiHYr04ZTe9FZvz25uefRK4T6QiLeOmf7wYFOkCgYEAwbz5
yE7Br8MXkQleUqolyB+BbpVfAh61/Ai5h8+12Z5i04AGlVmFg21IWp/MU6SMV2xX
aDmvBJWGPlvRfTc/bOoJvClPVfuX5WkzhxA5iD89UbCJzA6pQhDSNagt0rTEG/mf
HunkPmaLH01eQioHqYVEky/CJC3ORk6t+PPHKWkCgYAPSM17udcRag+P6s4/S8ef
cGMY97z4RdnBDy/YIyBajfKLxh/vSUxkYsPqWLSBkjdBgbvYkFuHg4Y0soUrimPB
3kBz/cIQ2hwnHCoHfJpKR4UiRk1qbFmCkE7s4BnJnhc0dhlEvGlqnYmmJGropc45
sNHJGFjceATNH9oTsyFWmQKBgDH9Hr4uhA9j2VrU/f96Y5FFf9lWvJMBdZd4cNa4
I4XpNjq4V/qFRMvqkLbBcKlMVeHg1JTR/XTDWAYTDvSuIrFpmeVxC0V2S3UoNeFt
sEqVdq7zTDrYtZeUW4j4wgoSFl/ZgtMpKnlnYBJNljqgOaXl+xG3SvKm1wiRGJaZ
4BOxAoGBAJ8+QPIighJ5xw2x/LXesaEkwBwgcq5UXHNUMTD9FMR2FyCR2dS+S/Kk
XVcU5jdu3Kan3OMdLImqmKPdpQdjx7JECHoHPoy7M5zaeC5Ug9564Dh17qMc+PB4
KyB/8/CxBdiDZN1wis8Q0yUasBIyxtuwp3PMLZV4KjxmenhsYfJi -----END RSA PRIVATE KEY----- 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 -----BEGIN CERTIFICATE-----
MIIDoTCCAomgAwIBAgIJANtsP/yFCr5eMA0GCSqGSIb3DQEBCwUAMGYxCzAJBgNV
BAYTAkNOMRAwDgYDVQQIDAdCZWlKaW5nMRAwDgYDVQQHDAdCZWlKaW5nMQ4wDAYD
VQQKDAVpS3VhaTEOMAwGA1UECwwFaUt1YWkxEzARBgNVBAMMCmlrdWFpOC5jb20w
IBcNMjEwNDIxMDcyMzA1WhgPMzAyMDA4MjIwNzIzMDVaMGYxCzAJBgNVBAYTAkNO
MRAwDgYDVQQIDAdCZWlKaW5nMRAwDgYDVQQHDAdCZWlKaW5nMQ4wDAYDVQQKDAVp
S3VhaTEOMAwGA1UECwwFaUt1YWkxEzARBgNVBAMMCmlrdWFpOC5jb20wggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC2+e+SLdxW9s+aodsZEOE1SXX6BhWr
mc1ZOFkbREepStWBbloUPdkzyXBLHCnfE0tGotZHlIRxdnkgkYxKarPlnUE6qT1i
xlyXY2RLVOI7xiJ1GKoRtZY+QI725GzKhydCuJ3UGTDIaLZxSccSXbgQjMffzovV
h7bheBHzZYyBdrvZKZkdSPA3QTVi+bF03V7h1SexGuEMvmbGKI1N+Ofl3P8f6FFm
CkatMoxdSwDqP2ah/LHBVHE/Kz60s9lMpVUfSnQsOC0rkXlxYjOgV15ZVoLCqQbI
x82eVd2T4ZNSlcregVcU90S4uoYJH03f+AwN2UPGcE3ZxodTiM1tWOSRAgMBAAGj
UDBOMB0GA1UdDgQWBBRxyUUUPYRZ0XgLcQQ5UtMInrZfmzAfBgNVHSMEGDAWgBRx
yUUUPYRZ0XgLcQQ5UtMInrZfmzAMBgNVHRMEBTADAQH/MA0GCSqGSIb3DQEBCwUA
A4IBAQArzw97JNQn3KS1Vt7d8EwXE83FgPfVv1/n+U25XktID9j0zcEsYUmfLqvE
0i1Trz2tRx+qHBAFVT3QE7p5uTaGQce3IA17oKzCGiioWg74QCUeuigw1MkmWUdE
qE6y1jllQ28U9QlWf+03B+mkoJOm+H1zze7UrvUck9BUmPLEWcw1QWT+CF1KrxJd
EuudxREu54i+IBl/8qISxdlWnQCIHP5iCEBjviU1G9n2mMS67krGWCGFnhRe19ir
t9CCztcqwEXTeKKEb4n++rp31MXcir1KIXJ7TGW3AEo329hCcF+FCYYOj85gQii2

Kt2h4VtX/upm3aPNpJNpTQogmzDW -----END CERTIFICATE-----

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/ikntpget
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:1BKY7uz3G$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$9.EU8ItY$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.