Documento conjunto LACNOG-M3AAWG: Melhores Práticas Operacionais Atuais sobre Requisitos Mínimos de Segurança para Aquisição de Equipamentos para Conexão de Assinante (CPE) LAC-BCOP-1

Maio 2019

Este documento está disponível no site do LACNOG em www.lacnog.net/docs/lac-bcop-1

Este documento está disponível no site do M3AAWG em www.m3aawg.org/CPESecurityBP-Portuguese

A versão original em Inglês está disponível no site do M3AAWG em www.m3aawg.org/CPESecurityBP

Este é um documento conjunto de Melhores Práticas Operacionais Atuais (*Best Current Operational Practices,* BCOP) desenvolvido pelo LACNOG[1] (Grupo de Operadores de Redes da América Latina e o Caribe) e pelo M3AAWG[2] (Messaging, Malware and Mobile Anti-Abuse Working Group). É o produto das versões originais do LACNOG por seus grupos de trabalho LAC-AAWG[3] (Grupo de Trabalho Antiabuso da América Latina e o Caribe) e Grupo de Trabalho BCOP[4], em cooperação com membros do M3AAWG, Assessores Técnicos Sêniores e o Comitê Técnico do M3AAWG.

Índice

1 Grupo de Operadores de Redes da América Latina e o Caribe (LACNOG), https://www.lacnog.net/
2 Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG), https://www.m3aawg.org/
3 Grupo de Trabalho Antiabuso da América Latina e o Caribe (LAC-AAWG), https://www.lacnog.net/lac-aawg/
4 Grupo de trabalho BCOP, https://www.lacnog.net/wg-bcops/

Sumário Executivo

CPE (do inglês *Customer Premise Equipment*) é o equipamento utilizado para conectar assinantes à rede de um Provedor de Serviços de Internet (*Internet Service Provider* – ISP). Exemplos de CPE incluem modems (cabo, xDSL, fibra) e roteadores WiFi, entre outros.
Devido a vulnerabilidades no *software* embarcado e nas configurações padrão, os CPEs têm sido alvo de uma variedade de abusos, que vão desde a exploração de serviços mal configurados e de credenciais de autenticação padrão, até o completo comprometimento por *malware*. O objetivo de muitos desses ataques é conduzir ataques de negação de serviço (DoS), mineração não autorizada de criptomoeda, propagação de *malware*, envio de *spam*, *phishing*, furto de credenciais e outros abusos.

Em geral, as vulnerabilidades comuns incluem:

- Credenciais padrão para um grande número de dispositivos
- Credenciais que não podem ser alteradas (*hard-coded*)
- Uso de protocolos e algoritmos obsoletos e inseguros
- Acessos não documentados (*backdoors*)
- Falta de mecanismo de atualização automatizado e seguro para tratar problemas de segurança
- Serviços desnecessários e/ou inseguros ativados por padrão
- Serviços que não podem ser desativados
- Gerenciamento remoto inseguro

Este documento destina-se a identificar um conjunto mínimo de requisitos de segurança que devem ser especificados quando os ISPs adquirem CPE, para propiciar que tais equipamentos tenham uma configuração padrão de fábrica segura e que permitam gerência e atualizações remotas. O objetivo é reduzir o risco de comprometimento das redes dos provedores, e da Internet como um todo, e minimizar os custos e impactos resultantes de abuso dos equipamentos por atacantes, tais como degradação ou indisponibilidade de serviços, suporte técnico e trabalho de reparo.

Está fora do escopo deste documento fornecer um conjunto completo de recursos ou as especificações de *hardware* e *software* que o CPE deve suportar[5]. Para o propósito deste documento, assume-se que os protocolos IPv6 e IPv4 são suportados, implementados e habilitados.

1. Terminologia

Para fins deste documento:

1. *Customer Premise Equipment* (CPE): equipamento usado para conectar assinantes à rede do provedor de serviços de Internet (ISP). Nomes diferentes podem ser usados por outros para descrever esse tipo de dispositivo, tais como Roteador da Borda do Cliente (*Customer Edge* - CE) e *Gateway* Residencial (*Residential Gateway* - RG).

2. *Firmware*: o *software* executado no CPE, incluindo o sistema operacional, podendo também incluir *software* de interface de rede, pacotes de *software* e serviços e configurações.

3. *Backdoor*: qualquer mecanismo inserido no sistema com o objetivo de permitir o acesso não documentado ao sistema ou aos seus dados. Exemplos de *backdoors* incluem um nome de usuário não documentado e inalterável (*hard-coded*), sem senha, com uma senha fixa ou "senha do dia" previsível,

5 Não incluir requisitos relativos ao suporte e implementação de IPv6 como parte da especificação de compra de CPE pode resultar em um risco de negócio para os ISPs, pois eles podem não ser capazes de fornecer conectividade IPv6 aos seus clientes. Isso representa um risco ao crescimento do negócio para o ISP devido ao esgotamento de endereços IPv4.

ou serviços não documentados para executar funções administrativas sem autenticação, entre outros. Um *backdoor* pode ser incluído intencionalmente (projetado para garantir o acesso posterior) ou acidentalmente (usado para fins de desenvolvimento e inadvertidamente incluído no *firmware* de produção). *Backdoors* também podem surgir como consequência de más práticas de programação.

4. Cifragem/Criptografia apropriada: algoritmos/protocolos criptográficos de padrão aberto publicados pelo Internet Engineering Task Force (IETF) ou outras organizações de padronização, em suas versões atuais. A implementação deve permitir a seleção de conjuntos de cifras e tamanhos de chave atualizados.

5. Credenciais inalteráveis (*hard-coded*): credenciais com valores comuns fixados no código-fonte do produto (o mesmo para todas as instalações do produto) que não podem ser alteradas ou desabilitadas, exceto pela correção do código-fonte (e, consequentemente, produzindo um novo binário/*firmware*).

6. Serviço (processo do tipo servidor ou *daemon*): um processo servidor que está ativamente aguardando conexões em uma porta específica, não o *software* cliente que faz consultas a um serviço, quando necessário.

7. PADRÃO (DEFAULT): uma configuração padrão de fábrica.

8. As palavras-chave "DEVE" ("MUST"/"SHALL"), "NÃO DEVE" ("MUST NOT"/"SHALL NOT"), "NECESSÁRIO" ("REQUIRED"), "DEVERIA" ("SHOULD"), "NÃO DEVERIA" ("SHOULD NOT"), "RECOMENDADO" ("RECOMMENDED"), "NÃO RECOMENDADO" ("NOT RECOMMENDED"), "PODE" ("MAY") e "OPCIONAL" ("OPTIONAL") neste documento devem ser interpretadas como descrito na BCP 14 RFC 2119 [2], e RFC 8174 [3] quando, e somente quando, elas aparecerem em letras maiúsculas, como mostrado neste parágrafo.

2. Requisitos Gerais (*General Requirements* – GR)

GR-01: A descrição do dispositivo DEVE incluir a identificação completa de seus componentes principais, em particular:

a. Fabricante, versões do modelo e do *chipset*
b. Nome, versão e data de lançamento do *firmware* e do sistema operacional de base

GR-02: O fornecedor DEVE prover documentação que descreva, no mínimo:

a. Nome, versão, data de lançamento e funcionalidade do *firmware* ou sistema operacional
b. Nome, versão, data de lançamento e estado de inicialização de fábrica (por exemplo, ativado ou desativado por padrão) de todos os aplicativos e serviços instalados no dispositivo

GR-03: O fornecedor DEVE prover as seguintes informações para qualquer *software* de código aberto utilizado:

a. Lista de todas as licenças relevantes para cada *software* de código aberto usado
b. nome completo e versão de cada *software* de código aberto incorporado ao sistema do CPE

GR-04: Informações de contato para divulgação de vulnerabilidades (VR-03) DEVERIAM ser incluídas em algum ponto (por exemplo, página, guia, etc.) da interface gráfica de usuário (*Graphical User Interface* - GUI) do CPE.

GR-05: O fornecedor DEVERIA prover informações ao usuário se o CPE está fora do período de suporte (consulte VR-01 e VR-02) e não recebe mais atualizações de *firmware* (por exemplo, por meio da interface gráfica de usuário).

3. Requisitos de Segurança de *Software* (*Software Security Requirements* – SSR)

SSR-01: Credenciais NÃO DEVEM ser inalteráveis (*hard-coded*). Veja também FR-04 e FR-05.

SSR-02: Os dados sensíveis de credenciais (por exemplo, senhas, chaves e *tokens* de segurança) armazenados no dispositivo DEVEM ser protegidos por algoritmos de *hash*/criptográficos apropriados. Chaves criptográficas DEVERIAM ser armazenadas em *hardware* seguro, se disponível.

SSR-03: Dados gerais armazenados no dispositivo DEVERIAM ser protegidos por criptografia apropriada.

SSR-04: Quaisquer ferramentas de *software* ou *backdoors* usados para o desenvolvimento de *firmware* ou sistema DEVEM ser removidos na versão de produção.

4. Requisitos de Atualização e Gerenciamento (*Update and Management Requirements* – MR)

MR-01: O CPE DEVE implementar um mecanismo para gerenciamento remoto que contemple, no mínimo, administração remota usando um protocolo de criptografia apropriado. Verifique a tabela no Anexo I para a lista de protocolo(s) necessário(s).

MR-02: O CPE DEVE implementar um mecanismo para atualização remota segura. Verifique a tabela no Anexo I para obter a lista de protocolo(s) necessário(s).

MR-03: Os mecanismos de gerenciamento e administração, e de atualização remotos DEVEM suportar:

a. Autenticação segura, e
b. Conexões criptografadas, e
c. Restrições de acesso para limitar conexões a origens específicas (por exemplo, segmentos de rede selecionados, uma URL específica etc.), e
d. A capacidade de escolher a porta de conexão (ou seja, suportar a alteração do número da porta PADRÃO/porta atribuída para o serviço [17]).

MR-04: No caso de atualização automatizada e segura, um mecanismo DEVE ser implementado para autenticar e validar o repositório fonte.

MR-05: O CPE DEVE implementar um mecanismo para verificar – antes de prosseguir com a atualização efetiva (tipicamente na memória flash) - a integridade e a autoridade do arquivo baixado e se ele é destinado para esse dispositivo (por exemplo, se é destinado à arquitetura, modelo, versão do dispositivo, etc.)

MR-06: O processo de atualização DEVE preservar as configurações existentes. O fornecedor PODE alterar uma configuração existente se essa alteração melhorar a segurança do dispositivo. Essa mudança DEVE ser claramente documentada.

MR-07: Em relação a verificações de atualizações, o CPE:

a. DEVE ter a capacidade de executar verificações periódicas para obter (*pull*) atualizações de forma automatizada e programada;
b. DEVE permitir que o usuário inicie a verificação de atualizações.

c. DEVERIA suportar as atualizações solicitadas pelo ISP sob demanda (*push*).

MR-08: O CPE DEVE implementar mecanismos para evitar sua inutilização como resultado de falha na atualização do *firmware* (*bricking*). Os procedimentos de recuperação DEVEM ser claramente documentados e NÃO DEVEM requerer o acesso a partes internas do *hardware*.

5. Requisitos Funcionais (*Functional Requirements* – FR)

Este documento pressupõe que o suporte a IPv6 de acordo com o RFC 7084 [8] faz parte do documento geral de requisitos de compra.

Esses recursos devem ser suportados ou removidos do CPE:

FR-01: O CPE NÃO DEVE ativar POR PADRÃO na interface WAN, serviços que permitam a divulgação de informações sensíveis ou que possam ser abusados para realizar ataques de amplificação (por exemplo, Telnet, FTP, SOCKS, CHARGEN, SNMP, etc.)

FR-02: O CPE DEVE implementar as funcionalidades de atualização remota e gerenciamento remoto, conforme descrito na sessão Requisitos de Atualização e Gerenciamento (Update and Management Requirements – MR) deste documento.

FR-03: Qualquer comunicação de gerenciamento do usuário final a partir da LAN/WLAN para o CPE DEVE ser autenticada[6] e DEVERIA ser criptografada.

FR-04: Qualquer informação de autenticação (por exemplo, senhas) DEVE ser alterável, incluindo a senha de administração geral (*root*). Os identificadores de usuários (por exemplo, nome de usuários) DEVERIAM ser alteráveis.

FR-05: Em relação à senha para acessar interfaces administrativas:

a. A senha inicial DEVE ser única para cada dispositivo e NÃO DEVE ser derivada de informações que possam ser obtidas por meio da captura de pacotes ou de métodos semelhantes de observação (por exemplo, endereço MAC);
b. A qualquer momento, quando uma senha é alterada ou redefinida (*reset*), a senha NÃO DEVE ser nula (ou seja, vazia, em branco) nem igual ao nome de usuário, e boas práticas relevantes para complexidade da senha DEVEM ser seguidas.

FR-06: O *firmware* de produção NÃO DEVE ter nenhum mecanismo não documentado para acessar o sistema ou seus dados.

FR-07: O dispositivo NÃO DEVE ter mecanismos de comunicação não documentados para enviar dados ao fornecedor ou a terceiros. Quaisquer comunicações e dados enviados ao fornecedor ou a terceiros DEVEM ser explicitamente documentados[7].

FR-08: Um usuário final autenticado DEVE ser capaz, por meio da interface gráfica do usuário:

a. De alterar as configurações específicas do usuário conforme apropriado (por exemplo, nome da rede WiFi, regras de *firewall*/encaminhamento, etc.), e

6 O CPE pode suportar mecanismos alternativos de autenticação para oferecer um nível mais alto de segurança do que simplesmente nome de usuário/senha.

7 Legislações de proteção de dados em muitos países/regiões podem impor requisitos especiais ao processamento de dados pessoais, exigindo que sejam detalhados e explicitamente documentados.

b. De desativar qualquer serviço que não seja essencial para a operação ou administração do dispositivo.

FR-09: Ao habilitar a operação de serviços para usuários na(s) interface(s) LAN/WLAN do CPE, tais serviços NÃO DEVEM ser acessíveis a partir da WAN/Internet, em particular serviços como DNS, NTP, SSDP, UPnP, ou qualquer outro protocolo que possa ser usado em ataques de amplificação.

FR-10: Para usar um serviço/agente de monitoramento e/ou gerenciamento:

a. A configuração de um mecanismo de autenticação apropriado para definir valores e/ou para recuperar informações/dados sensíveis DEVE ser necessária;

b. O acesso a partir de interface(s) WAN DEVE usar autenticação e DEVE ser restrito a origens específicas (por exemplo, a um segmento ou endereço de rede selecionado).

FR-11: O dispositivo DEVE implementar métodos criptográficos baseados em padrões abertos em suas versões atuais, que permitem a seleção de parâmetros seguros em relação ao conjunto de cifras e tamanho das chaves.

FR-12: Serviços criptográficos ou aplicações que envolvam a geração de chaves e/ou certificados digitais para autenticação de dispositivos DEVEM gerar as chaves para cada dispositivo; ou seja, uma chave privada NÃO DEVE ser compartilhada entre diferentes dispositivos.

FR-13: O CPE DEVE suportar a sincronização de tempo por meio de um protocolo de tempo centralizado, como o *Network Time Protocol* (NTP). Apenas o *software* cliente NTP é necessário. O CPE NÃO DEVE ter uma configuração inalterável (*hard-coded*) para os servidores NTP e NÃO DEVE usar POR PADRÃO servidores para os quais o fornecedor não tenha permissão de uso.

FR-14: O CPE DEVERIA suportar a RFC 6092 "Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service"[6]. No caso de um conflito entre a RFC 6092 e este documento, o requisito deste documento prevalecerá.

FR-15: O CPE DEVE suportar filtragem *antispoofing* de acordo com a BCP 38 RFC 2827 [12] para ambos os protocolos, IPv4 e IPv6. DEVE ser uma opção selecionável, ativa POR PADRÃO. Está fora do escopo deste documento determinar a técnica a ser usada para validação do endereço IP de origem.

FR-16: O CPE DEVERIA suportar a filtragem de pacotes para endereços IP reservados para propósito específico (*Special-Purpose Address*). Endereços considerados "Globally Reachable" FALSE E "Forwardable" FALSE, de acordo com a RFC 6890 [13] e RFC 8190 [14], DEVERIAM ser filtrados. Neste caso, o CPE DEVERIA ser capaz de aceitar configuração para incluir endereços IPv4 e IPv6 de acordo com os registros mantidos pela IANA (Internet Assigned Numbers Authority), como descrito em "IANA IPv4 Special-Purpose Address Registry" [15] e "IANA IPv6 Special-Purpose Address Registry" [16].

FR-17: O CPE NÃO DEVE atuar como um servidor DNS recursivo aberto. Em relação a serviços DNS:

a. As consultas DNS recebidas na porta WAN e destinadas ao próprio CPE NÃO DEVEM ser permitidas ou respondidas.

b. As consultas DNS recebidas na porta WAN e destinadas a serem encaminhadas pela porta LAN PODEM ser permitidas, desde que exista uma regra explícita para isso na configuração do CPE (por exemplo, regra de encaminhamento, regra de *firewall* etc.).[8]

c. Se o CPE estiver executando um servidor DNS local, ele DEVERIA marcar as consultas DNS de saída (*outbound*) para executar a validação DNSSEC.

d. Se o CPE não estiver executando um servidor DNS local e, em vez disso, estiver encaminhando consultas DNS para outro servidor, então ele NÃO DEVE remover marcações de validação DNSSEC das consultas DNS se elas existirem.

FR-18: Quando WiFi é provido, o CPE:

a. DEVE implementar mecanismos de segurança com criptografia apropriada.

b. DEVERIA suportar a versão mais recente da especificação de recursos de segurança *Wi-Fi Protected Access (WPA)* ®.

FR-19: As senhas NÃO DEVEM ser visíveis em texto claro POR PADRÃO em nenhuma interface de gerenciamento. Senhas PODEM tornar-se visíveis quando solicitado pelo usuário.

FR-20: Um método para fazer *download* da configuração do dispositivo em formato de texto puro (ASCII ou UTF-8) DEVERIA existir, contanto que todas as informações sensíveis (por exemplo, senhas, *strings* de comunidade, etc.) sejam editadas (*redacted*) da saída (*output*).

6. Requisitos de Configuração Inicial (*Initial Configuration Requirements* – IR)

Os dispositivos DEVEM ter as seguintes configurações padrão de fábrica:

IR-01: O CPE DEVE ser configurado de forma restritiva, ao invés de ser configurado de forma permissiva. Todos os serviços (processos do tipo servidor) que não são estritamente necessários para o processo de configuração inicial (*bootstrapping*) DEVEM estar desativados, especialmente (se implementado) SSDP, SNMP, UPnP, SOCKS, SMB, teste de largura de banda (ergo *imbedded* iperf e outros). Além disso, os serviços que estão habilitados ou podem ser ativados DEVERIAM operar em um modo padrão restritivo e/ou seguro.

IR-02: Parâmetros relacionados a endereços de servidores DNS (*resolver addresses*) DEVEM estar desconfigurados e a opção de *DNS Relay* (se implementada) DEVE estar desativada.

IR-03: O encaminhamento de porta (*port forwarding*) ou a opção de *host DMZ*, se disponíveis, DEVEM estar desativadas POR PADRÃO.

IR-04: A senha inicial para acessar interfaces administrativas, tanto gráficas quanto de linha de comando, DEVE ser única para cada dispositivo e DEVE ser possível identificá-la visualmente na etiqueta do dispositivo.

IR-05: Quando o WiFi é provido, a(s) rede(s) WiFi DEVE(M) ter uma senha inicial única, NÃO igual ao SSID, e DEVE ser possível identificar a(s) senha(s) inicial(is) visualmente na etiqueta do dispositivo. A(s) senha(s) DEVERIA(M) ser diferente(s) da senha PADRÃO de administração.

IR-06: Quando o WiFi é provido, o(s) valor(es) PADRÃO do(s) *Service Set Identifier(s)*(SSIDs) NÃO DEVE(M) estar relacionado(s) ao nome do fornecedor nem ao modelo do produto e DEVE(M)

8 O CPE não deveria impedir o usuário de hospedar um servidor DNS na LAN. Vale ressaltar, neste caso, que uma regra de encaminhamento/firewall só faz sentido se um servidor de DNS autoritativo estiver em execução na LAN.

ser customizável(eis). Verifique a tabela no Anexo I para valores PADRÃO personalizados pelo ISP[9].

IR-07: No caso do serviço SSH, o par de chaves do servidor NÃO DEVE ser pré-gerado na fábrica. A chave DEVE ser gerada após a primeira inicialização/*boot* do serviço e qualquer reinicialização (*reset*) de fábrica deve fazer com que uma nova chave seja gerada. O par de chaves gerado deve prover bits suficientes para ser considerado seguro no momento da implementação.

IR-08: A filtragem *antispoofing* [FR-15] DEVE estar ativada POR PADRÃO.

IR-09: Mecanismos de transição IPv6, túneis, VPNs e serviços similares DEVEM estar desativados POR PADRÃO.

7. Requisitos do Fornecedor (*Vendor Requirements* – VR)

O fornecedor:

VR-01: DEVE ter uma política clara de suporte ao produto, especialmente em relação à disponibilidade de correções para vulnerabilidades de segurança, incluindo o período após a data de término de venda (*end-of-sale date*).

VR-02: DEVE fornecer correções para vulnerabilidades de segurança no mínimo enquanto o dispositivo está à venda. O fornecedor DEVERIA continuar fornecendo correções de segurança por 3 (três) anos a partir da data de término da venda (*end-of-sale date*).

VR-03: DEVE possuir uma capacidade de divulgação de vulnerabilidades de forma coordenada, incluindo um canal de comunicação/ponto de contato que permita que ISP clientes, usuários finais e terceiros (como pesquisadores) relatem vulnerabilidades de segurança descobertas no(s) produto(s). Idealmente, DEVERIA ter uma equipe de resposta a incidentes de segurança de produto (*Product Security Incident Response Team* - PSIRT).

VR-04: DEVE ter um canal de suporte publicamente disponível que não exija registro prévio ou uma conta de usuário, no mínimo, por meio de um *site Web* em inglês para:

a. Informar sobre vulnerabilidades existentes, medidas de mitigação e correções de segurança associadas ao(s) seu(s) produto(s);
b. Prover correções de segurança e/ou novas versões de *firmware* ou *software* para seu(s) produto(s);
c. Fornecer manuais e outros materiais relacionados à configuração, atualização e segurança do dispositivo.

8. Lista de Acrônimos

BCOP: Best Current Operational Practices

BBF: Broadband Forum

CE: Customer Edge Router

CPE: Customer Premises Equipment

[9] Caso o ISP queira escolher como os SSIDs serão nomeados POR PADRÃO (por exemplo, um único nome para todos os dispositivos ou nomes exclusivos por dispositivo), o ISP precisará descrever como os SSIDs DEVEM ser nomeados. Caso contrário, o fornecedor pode escolher o PADRÃO.

CWMP: CPE WAN (Wide Area Network) Management Protocol

IANA: Internet Assigned Numbers Authority

ISP: Internet Service Provider

PSIRT: Product Security Incident Response Team

RG: Residential Gateway

SSID: Service Set Identifier

WLAN: Wireless LAN (Local Area Network)

9. Agradecimentos

Muitas pessoas contribuíram para o desenvolvimento deste documento, desde seu início no Grupo de Trabalho Antiabuso da América Latina e o Caribe (LAC-AAWG) até a sua publicação.

Os autores gentilmente agradecem a todos os colaboradores por suas muitas sugestões úteis, em alguns casos fornecendo uma revisão detalhada. Colaboradores (em ordem alfabética de sobrenome) incluem: Nicolas Antoniello, John Brown, Dennis Dayman, Carmen Denis, Yuri Ferreira, Alexandre Giovaneli, Steve Goeringer, Cristine Hoepers, Markus Lintula, Jason Livingood, Art Manion, Jordi Palet Martínez, Roney Medeiros, Luciano Minuchin, Eduardo Barasal Morales, Massimiliano Pala, Ricardo Patara, Nathalia Sautchuk Patrício, Fernando Quintero, Marcelo Batista Sarmento, Joe St Sauver, Klaus Steding-Jessen, Italo Valcy, Severin Walker, Ariel Weher, Gilberto Zorello, and Jan Žorž.

Agradecimentos especiais vão para:

- Lucimara Desiderá, cofundadora e coordenadora do LAC-AAWG, autora/editora
- Christian O'Flaherty, cofundador e coordenador do LAC-AAWG
- A comunidade e o coordenador do Grupo de Trabalho BCOP do LACNOG por apoiar o desenvolvimento e o processo de revisão do documento
- O LACNIC WARP (*Warning Advice and Reporting Point*) do Registro de Endereçamento da Internet para a América Latina e o Caribe (LACNIC) por fornecer infraestrutura para as reuniões presenciais
- O Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) por apoiar a iniciativa LAC-AAWG e aceitar este documento para revisão técnica.

10. Referências Informativas

[1] Abuse of Customer Premise Equipment and Recommended Actions
https://resources.sei.cmu.edu/asset_files/WhitePaper/2014_019_001_312679.pdf

[2] Key words for use in RFCs to Indicate Requirement Levels, BCP 14, RFC 2119
http://www.rfc-editor.org/info/rfc2119

[3] Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words, RFC 8174
https://tools.ietf.org/html/rfc8174

[4] Internet Security Glossary, Version 2, RFC 4949
https://tools.ietf.org/html/rfc4949

[5] Common Security Requirements for IP-Based MSO-Provided CPE - Version I01
https://apps.cablelabs.com/specification/common-security-requirements-for-ip-based-mso-provided-cpe

[6] Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service, RFC 6092
https://tools.ietf.org/html/rfc6092

[7] Data-Over-Cable Service Interface Specifications DOCSIS® 3.1, Security Specification, CM-SP-SECv3.1-I07-170111
https://apps.cablelabs.com/specification/CM-SP-SECv3.1

[8] Basic Requirements for IPv6 Customer Edge Routers, RFC 7084
https://tools.ietf.org/html/rfc7084

[9] Functional Requirements for Broadband Residential Gateway Devices, TR-124 Issue 5
https://www.broadband-forum.org/technical/download/TR-124_Issue-5.pdf

[10] CPE WAN Management Protocol, TR-069 Issue 1 Amendment 6
https://www.broadband-forum.org/technical/download/TR-069.pdf

[11] IPv4 and IPv6 eRouter Specification CM-SP-eRouter-I19-160923
https://apps.cablelabs.com/specification/ipv4-and-ipv6-erouter-specification/

[12] Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, BCP 38, RFC 2827
https://tools.ietf.org/html/rfc2827

[13] Special-Purpose IP Address Registries, BCP 153, RFC 6890
https://tools.ietf.org/html/rfc6890

[14] Updates to the Special-Purpose IP Address Registries, BCP 153, RFC 8190
https://tools.ietf.org/html/rfc8190

[15] IANA IPv4 Special-Purpose Address Registry
https://www.iana.org/assignments/iana-ipv4-special-registry

[16] IANA IPv6 Special-Purpose Address Registry
https://www.iana.org/assignments/iana-ipv6-special-registry

[17] Service Name and Transport Protocol Port Number Registry
https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

[18] Addressing the challenge of IP spoofing
https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-AntiSpoofing-20150909-en-2.pdf

[19] ISO/IEC 29147:2014 Information technology - Security techniques - Vulnerability disclosure
https://standards.iso.org/ittf/PubliclyAvailableStandards/c045170_ISO_IEC_29147_2014.zip

[20] BSI TR-03148: Secure Broadband Router
Requirements for a secure Broadband Router Version: 1.0
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03148/TR03148.pdf?__blob=publicationFile&v=2

Anexo 1 – Tabela de Requisitos

A tabela a seguir resume o conjunto de requisitos apresentados neste documento e destina-se a ajudar as organizações (por exemplo ISPs) a prepararem RFPs ou especificarem os requisitos que desejam dos fornecedores.

Alguns campos já estão preenchidos com a seleção recomendada, especialmente quando o requisito é obrigatório, mas uma boa parte dos requisitos exige que a organização decida se deseja uma determinada configuração ou não e defina sua configuração PADRÃO.

Vale ressaltar que os itens indicados neste documento são um conjunto mínimo de requisitos de segurança e é altamente recomendável que as escolhas não sejam rebaixadas a algum nível menos rigoroso (por exemplo, de implementação mandatória para recomendada ou opcional). Sempre que possível, elas deveriam ser elevadas para a opção mais rigorosa.

Requisitos Gerais (GR)		
Requisito	**M Mandatório R Recomendado O Opcional**	**Configuração PADRÃO**
GR-01	M	
GR-02	M	
GR-03	M	
GR-04	R	Informação de contato para divulgação de vulnerabilidades disponível na interface gráfica do usuário
GR-05	R	Estado atual quanto a atualizações
Requisitos de Segurança de *Software* (SR)		
Requisito	**M Mandatório R Recomendado O Opcional**	**Configuração PADRÃO**
SSR-01	M	
SSR-02	M	Dados sensíveis protegidos
SSR-03	R	
SSR-04	M	Ferramentas de desenvolvimento de *software* e/ou *backdoors* removidos

Requisitos de Atualização e Gerenciamento (MR)		
Requisito	**M Mandatório R Recomendado O Opcional**	**Configuração PADRÃO**
MR-01	M (a)	(a)
MR-02	M (b)	(b)
MR-03	a. M b. M c. M d. M	(c)
MR-04	M	
MR-05	M	
MR-06	M	
MR-07	a. M b. M c. R	
MR-08	M	
Requisitos Funcionais (FR)		
Requisito	**M Mandatório R Recomendado O Opcional**	**Configuração PADRÃO**
FR-01	M	Telnet, FTP, SOCKS, CHARGEN, SNMP desativados
FR-02	M	(c)
FR-03	DEVE autenticar e é RECOMENDADO para criptografar.	
FR-04	M	
FR-05	a. M b. M	Senha inicial única por dispositivo
FR-06	M	
FR-07	M	
FR-08	a. M b. M	

FR-09	M	DNS, NTP, SSDP, UPnP não acessível a partir da WAN
FR-10	a. M b. M	(d)
FR-11	M	
FR-12	M	
FR-13	M	Apenas cliente NTP. Nenhuma configuração inalterável (*hard-coded*).
FR-14	R	
FR-15	M	Filtragem *antispoofing* ativada
FR-16	R	Desconfigurado (e)
FR-17	a. M b. R c. R d. M	b. Nenhuma regra de encaminhamento ativada
FR-18	a. M b. R	Criptografia apropriada ativada
FR-19	M	
FR-20	R	

Requisitos de Configuração Initial (IR)

Requisito	**M Mandatório** **R Recomendado** **O Opcional**	**Configuração PADRÃO**
IR-01	M	SSDP, SNMP, UPnP, SOCKS, SMB, teste de largura de banda desativados
IR-02	M	Nenhum endereço de servidor DNS predefinido e o DNS Relay desativado
IR-03	M	Desativadas
IR-04	M	(f)
IR-05	M	(f)
IR-06	M	(g)
IR-07	M	Nenhuma chave SSH pré-gerada
IR-08	M	Ativada

IR-09	M	Mecanismos de transição, túneis, VPN desativados
Requisitos do Fornecedor (VR)		
Requisito	**M Mandatório R Recomendado O Opcional**	**Configuração PADRÃO**
VR-01	M	
VR-02	M	
VR-03	M	
VR-04	M	

(a) O ISP deve ter a capacidade de gerenciar os dispositivos remotamente (por exemplo, para configuração). Dependendo da tecnologia usada pelo provedor (cabo, fibra, xDSL), o correspondente segmento da indústria pode ter protocolos já especificados. Neste item, o ISP precisa escolher o(s) protocolo(s) que devem ser suportados pelo dispositivo de acordo com sua tecnologia (por exemplo, BBF TR - 069 CWMP para banda larga), se ele deveria ser ativado POR PADRÃO e as configurações padrão necessárias. Se mais de um protocolo deve ser suportado, a organização precisa incluir todos eles.

(b) O ISP deve ter a capacidade de atualizar o dispositivo remotamente (principalmente o *firmware*). Dependendo da tecnologia usada pelo provedor (cabo, fibra, xDSL), o correspondente segmento da indústria pode ter protocolos já especificados. Neste item, a organização precisa escolher o(s) protocolo(s) que devem ser suportados pelo dispositivo de acordo com sua tecnologia (por exemplo, BBF TR - 069 CWMP para banda larga), se deveria ser ativado POR PADRÃO e as configurações padrão necessárias. Se mais de um protocolo deve ser suportado, a organização precisa incluir todos eles.

(c) Não utilizar mecanismos mínimos para controle de acesso, confidencialidade e verificação de integridade nas transações entre os CPEs e o servidor de gerenciamento/atualização pode frequentemente resultar no comprometimento da infraestrutura do provedor. É altamente recomendável usar conexão criptografada (por exemplo, TLS/HTTPS) para todo o acesso; usar autenticação não baseada em um nome de usuário/senha pré-definidos para todos os dispositivos; e restringir o acesso a fontes determinadas (por exemplo, para um segmento de rede selecionado, URL específica, etc.).

(d) Se o ISP quiser um serviço/agente de monitoramento e/ou gerenciamento habilitado por padrão, ele deve fornecer os parâmetros apropriados para autenticação e restrição de acesso via rede.

(e) Se o ISP quiser implementar diretamente no CPE a filtragem para endereços IP reservados para propósito específico, ele poderá fornecer a lista de prefixos que podem ser filtrados POR PADRÃO. Caso contrário, a configuração PADRÃO será "desconfigurada" e o CPE não aplicará nenhum filtro para tais prefixos.

(f) Se o ISP quiser personalizar como a senha inicial deve ser definida, o ISP precisa informar o fornecedor sobre o processo de seleção da senha. Caso contrário, o fornecedor pode definir valores únicos aleatórios como PADRÃO.

(g) Se o ISP quiser personalizar o(s) nome(s) da(s) rede(s) WiFi, ele precisará informar como os Identificadores de WiFi (SSIDs) devem ser configurados. Caso contrário, o fornecedor pode escolher o(s) valor(es) PADRÃO(ÕES).

Para todos documentos que publicamos, por favor, verifique o site do M3AAWG (www.m3aawg.org) ou o site do LACNOG (www.lacnog.net) para atualizações.

Esta tradução para o idioma Português é uma contribuição do CERT.br/NIC.br (www.cert.br)