DATACOM

DATACOM
SECURITY

VULNERABILITY NOTES

5 de fevereiro de 2026

Contatos

Suporte Técnico

A Datacom disponibiliza um portal de atendimento - DmSupport, para auxílio aos clientes no uso e configuração de nossos equipamentos.

O acesso ao DmSupport pode ser feito através do link: https://supportcenter.datacom.com.br

Neste portal estão disponíveis firmwares, descritivos técnicos, guia de configuração, MIBs e manuais para download. Além disto, permite a abertura de chamados para atendimento com a nossa equipe técnica.

Para contato telefônico: **+55 51 3933-3122**

Salientamos que o atendimento de nosso suporte por telefone ocorre de segunda a sexta-feira das 08:00 as 17:30.

Importante: Para atendimento de suporte em regime 24x7, favor solicitar cotação ao nosso setor comercial.

Informações Gerais

Para qualquer outra informação adicional, visite https://www.datacom.com.br ou entre em contato:

DATACOM

Rua América, 1000

92990-000 - Eldorado do Sul - RS - Brazil

+55 51 3933-3000

Introdução ao Documento

Este documento fornece informações relativas a vulnerabilidades de software nos produtos DATACOM. Ele descreve as vulnerabilidades corrigidas, seu impacto e solução adequada.

Público-Alvo

Este documento é direcionado para Engenheiros e Administradores de Rede, ou qualquer outra pessoa qualificada tecnicamente, responsável por configurar e manter equipamentos DATACOM.

Vulnerabilidades

Vulnerabilidade é uma fragilidade ou falha específica em um software, hardware ou sistema de rede que pode ser explorada por um invasor para comprometer sua segurança. As vulnerabildades aqui apresentadas nas famílias dos produtos Datacom são vulnerabilidades já corrigidas e que ocorreram devido a:

- Erro Humano
- Falhas de Projeto
- Problemas de Configuração
- Componentes de Terceiros

Este documento apresenta as informações das vulnerabilidades baseadas na seguinte convenção especificada pela ANATEL.

Referência (Requisito 7.12.1): https://informacoes.anatel.gov.br/legislacao/component/ content/article/164-atos-de-certificacao-de-produtos/2024/1992-ato-16417:

Item	Descrição
ID	Identificador exclusivo para cada comunicado.
Título	Referência genérica e sucinta referente ao(s) produto(s) afetado(s) e à vulnerabilidade corrigida.
Visão geral	Breve resumo de alto nível sobre a vulnerabilidade para que os usuários possam entender os pontos principais e determinar rapidamente se o aviso é aplicável ao seu ambiente.
Descrição	Descrição com mais informações que permitam aos usuários entenderem como são afetados e avaliarem sua exposição. Não deve fornecer detalhes a ponto de permitir a exploração da vulnerabilidade.
Produtos afetados	Uma lista de produtos afetados conhecidos e suas versões.
Impacto	Informações que descrevam o impacto da vulnerabilidade (por exemplo, negação de serviço, execução de códigos maliciosos) e a criticidade da vulnerabilidade por meio de sistema de pontuação de severidade reconhecido internacionalmente (ex.: Common Vulnerability Scoring System - CVSS).

Item	Descrição
Solução	Informações sobre a ação que os usuários devem realizar para corrigir ou remediar a vulnerabilidade e seu impacto.
Créditos	Reconhecimento ao descobridor (notificador) por relatar a vulnerabilidade e/ou outros envolvidos no processo de solução.
Histórico	Versão e data da publicação original. Pode conter um histórico de modificações se o boletim for atualizado posteriormente.

Referência (Requisito 7.12.1): https://informacoes.anatel.gov.br/legislacao/component/ content/article/164-atos-de-certificacao-de-produtos/2024/1992-ato-16417

Sumário

1 DmOS

As vulnerabilidades corrigidas nas versões do DmOS são apresentadas abaixo:

Item	Descrição
ID	CVE-2024-6387
Título	DmOS vulnerável a CVE-2024-6387 referente ao OpenSSH.
Visão geral	Existia uma condição de corrida que poderia levar o OpenSSH a lidar com alguns sinais de forma insegura. Um atacante remoto não autenticado poderia explorá-la ao falhar na autenticação dentro de um determinado período de tempo.
Descrição	Condições de corrida ocorrem frequentemente em manipuladores de sinais, devido as ações assíncronas suportadas. Ataques podem ser capazes de explorar uma condição de corrida em um manipulador de sinal para corromper o estado do produto, possivelmente levando a uma negação de serviço ou até mesmo a execução de código.
Produtos afetados	Produtos da linha DmOS.
Impacto	Possibilidade de acesso root por invasores não autenticados, que poderiam assumir o controle total dos produtos afetados.
Solução	Aplicado patch de segurança na própria versão do Openssh 8.8p1 evitando o DmOS a partir da versão 12.0.0 a ficar exposto a vulnerabilidade identificada pela CVE-2024-6387. Recomenda-se a atualização do firmware do produto para a versão 12.0.0 ou superior.
Créditos	Cliente Datacom
Histórico	27-JAN-2026

Item	Descrição
ID	B-243796
Título	Memory Leak causado por consulta SNMP.
Visão geral	Equipamento pode ficar sem memória quando há consultas SNMP em loop quando O switch não possuir configuração de BGP.
Descrição	Um memory leak ocorria no módulo responsável pelo BGP quando era executado um SNMPWALK e a configuração de BGP no switch não existia.
Produtos afetados	Switches da linha DmOS.
Impacto	Consumo de memória com sua não liberação ocasionando queda no sistema após longo período de uso.
Solução	Corrigido com a liberação dos recursos alocados na função do protocolo BGP. Recomenda-se a atualização do firmware do produto para a versão 10.6.0 ou superior.

Item	Descrição
Créditos	Cliente Datacom
Histórico	30-MAI-2025

Item	Descrição
ID	B-242531
Título	Processamento do Zabbix em 100%.
Visão geral	Limite de 5 sessões SNMP por padrão no DmOS gerava alto consumo de processamento por parte da ferramenta Zabbix.
Descrição	Ao incluir uma fila de CPU Protect para o protocolo SNMP com o valor 5, a ferramenta de monitoramento Zabbix teve seu processamento elevado para 100% devido ao processo de poller ficar sempre ocupado aguardando resposta dos switches DmOS.
Produtos afetados	Switches da linha DmOS.
Impacto	Não atendimento de todos os hosts e quebra nos gráficos da ferramenta Zabbix.
Solução	O valor padrão foi alterado de 5 para 16 sessões SNMP a partir da versão de firmware 10.4.4. Recomenda-se a atualização do firmware do produto para a versão 10.4.4 ou superior.
Créditos	Cliente Datacom
Histórico	23-ABR-2025

Item	Descrição
ID	B-231112
Título	Core-dump no nbase-stub após remoção de interface L3.
Visão geral	Ao remover interface L3 o software poderia gerar um Hard Assert ocasionando falhas no encaminhamento dos pacotes dos protocolos L3.
Descrição	Problema de corrupção de memória após a remoção de uma interface L3 gerava queda nos protocolos.O switch precisava ser reinicializado para retornar com a operação normal do produto.
Produtos afetados	Switches da linha DmOS.
Impacto	Queda nos tráfegos que dependiam dos protocolos L3.
Solução	Gerado patch com a correção da corrupção de memória a partir da versão de firmware 10.4.2. Recomenda-se a atualização do firmware do produto para a versão 10.4.2 ou superior.
Créditos	Cliente Datacom
Histórico	07-ABR-2025

2 ONU

Item	Descrição
ID	CVE-2022-27255
Título	Módulo SIP ALG vulnerável a buffer overflow nas ONUs DM986-414, DM986-414Q e DM986-204.
Visão geral	Vulnerabilidade poderá ser explorada através da execução de scripts gerando sobrecarga no sentido upstream da rede
Descrição	Vulnerabilidade no SIP ALG do SDK do chipset da família Realtek 819x, o qual possibilita um ataque remoto através da WAN ou da LAN ou possível corrompimento no sistema do produto.
Produtos afetados	DM986-414, DM986-414Q e DM986-204
Impacto	Corrompimento no produto ou ataques a partir do produto com forte consumo da banda disponível da rede no sentido upstream.
Solução	Atualizar o firmware/software do produto para a versão 8.0.0 da DM986-414, para a versão 5.0.0 da DM986-414Q e para a versão 4.0.0 da DM986-204.
Créditos	Fernando Frediani e demais Clientes Datacom
Histórico	03-OUT-2025

Nota Legal

Apesar de terem sido tomadas todas as precauções na elaboração deste documento, a DATACOM não assume qualquer responsabilidade por eventuais erros ou omissão bem como nenhuma obrigação é assumida por danos resultantes do uso das informações contidas neste guia. As especificações fornecidas neste manual estão sujeitas a alterações sem aviso prévio e não são reconhecidas como qualquer espécie de contrato.

Garantia

Os produtos da DATACOM possuem garantia contra defeitos de fabricação pelo período mínimo de 12 (doze) meses, incluído o prazo legal de 90 dias, a contar da data de emissão da Nota Fiscal de fornecimento.

Nossa garantia é padrão balcão, ou seja, para o exercício da garantia o cliente deverá enviar o produto para a Assistência Técnica Autorizada DATACOM, com frete pago. O frete de retorno dos equipamentos será de responsabilidade da DATACOM.

Para maiores detalhes, consulte nossa política de garantia no site https://www.datacom.com.br.

Para contato telefônico: **+55 51 3933-3094**