Correção da exposição de usuários no portal institucional

Relatório técnico à Câmara Municipal de Rochedo – MS
12 de novembro de 2026

A Digitar Informática corrigiu a falha que permitia identificar usuários do WordPress no portal cmrochedo.ms.gov.br. Com a correção, a consulta pública à API REST descrita na notificação deixou de expor os identificadores de usuários.

Registro da ocorrência

Data e hora do registro	30 de setembro de 2026, às 04:39:17 UTC
Ativo identificado	cmrochedo.ms.gov.br | IP 143.244.187.111
Serviço	WordPress | HTTPS na porta TCP 443
Referência da notificação	CVE-2017-5487

Exposição identificada e impacto

A API REST é a interface que o WordPress utiliza para responder a consultas de aplicações e outros serviços. Na ocorrência comunicada, um visitante conseguia obter identificadores de usuários sem iniciar sessão no portal. Essa possibilidade de descobrir quais contas existem é chamada de enumeração de usuários.

De posse de um identificador válido, um terceiro pode direcionar tentativas de autenticação a uma conta específica. A notificação descreve a exposição desses identificadores. Por si só, esse registro não comprova divulgação de senhas, acesso a contas ou alteração de conteúdo.

Alcance da correção

A medida corretiva tratou a informação que a aplicação disponibilizava a visitantes na consulta reportada. O critério de verificação dessa correção é que uma consulta feita sem autenticação já não permita identificar os usuários anteriormente expostos.

Docspaper - https://digitar.legissuper.com.br/validate/doc/signature/4b6abe92-6f04-4ecd-b80b-5970e6bea2b6
Docspaper - https://digitar.legissuper.com.br/validate/doc/signature/4b6abe92-6f04-4ecd-b80b-5970e6bea2b6

Controles de proteção do portal

O portal recebe tráfego público por HTTPS. Como essa conexão precisa estar disponível aos visitantes, a proteção envolve tanto o controle das conexões de rede quanto a inspeção das requisições que chegam à aplicação.

Firewall de borda. Filtra o tráfego no perímetro da rede, antes que ele alcance o servidor. As regras de entrada limitam as conexões aos destinos e serviços autorizados.

Firewall local com iptables. Aplica uma segunda filtragem no próprio servidor. As regras locais determinam quais conexões podem alcançar os serviços, considerando portas, protocolos e condições de tráfego.

ModSecurity. Inspeciona as requisições dirigidas à aplicação web e aplica as regras configuradas. Essa inspeção permite identificar ou bloquear padrões suspeitos mesmo quando a conexão utiliza uma porta autorizada, como a do portal.

Fail2Ban. Monitora os registros dos serviços protegidos. Quando tentativas malsucedidas de uma mesma origem atingem o limite configurado, o endereço IP pode ser bloqueado temporariamente, reduzindo a repetição dessas tentativas.

Disponibilidade e isolamento de recursos

Redundância. O ambiente dispõe de recursos alternativos para apoiar a continuidade do serviço em caso de falha de um dos componentes cobertos.

Isolamento de núcleos de processamento. A separação de recursos de CPU entre cargas de trabalho reduz a disputa por processamento. Assim, um aumento de demanda em uma carga tem menor impacto sobre a capacidade reservada às demais.

Parecer técnico

A Digitar Informática considera corrigida a exposição de identificadores pela consulta indicada na notificação. Para acompanhar esse ponto, recomenda-se repetir a verificação sem autenticação após atualizações do WordPress ou mudanças nas permissões da API REST.

Leandro Moraes Lino
Analista de Infraestrutura e Cyber Segurança

Docspaper - https://digitar.legissuper.com.br/validate/doc/signature/4b6abe92-6f04-4ecd-b80b-5970e6bea2b6
Docspaper - https://digitar.legissuper.com.br/validate/doc/signature/4b6abe92-6f04-4ecd-b80b-5970e6bea2b6

DOCS PAPER

CERTIFICADO DE ASSINATURA DIGITAL

Código do Documento: a6e5a90e-071d-4b74-bbb4-1b9258477a7c

RESUMO DAS ASSINATURAS:

JAISON COUTINHO - CNPJ 11.***.***/****-06 - Certificado digital - 12/11/2026, 18:04:31

ASSINATURAS:

Assinado por: JAISON COUTINHO **Certificado digital**

CNPJ 11.***.***/****-06

Assinado em: 12/11/2026, 18:04:31

Emissor: ICP-Brasil · Válido até: 30/09/2027, 09:27:39

Verifique a autenticidade deste documento em:

https://digitar.legissuper.com.br/validate/doc/signature/4b6abe92-6f04-4ecd-b80b-5970e6bea2b6

Este documento foi assinado digitalmente conforme a MP 2.200-2/2001.