BOLETIM DE SEGURANÇA

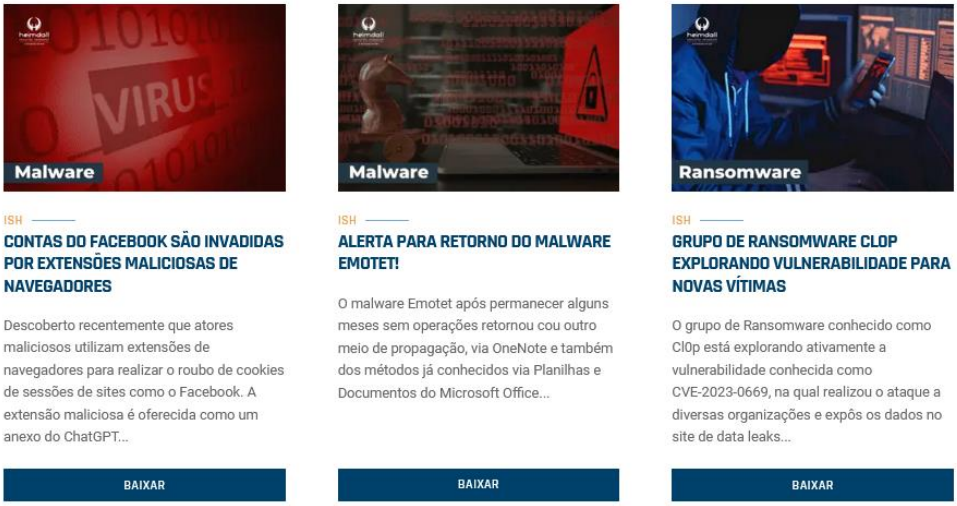
Vulnerabilidade grave no Linux é descoberta por EvilSocket

heimdall
security research
A DIVISION OF ISH

TLP: CLEAR

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall



SUMÁRIO

1 Sumário Executivo 4
2 Informações sobre a vulnerabilidade 5
3 Recomendações 7
4 Referências 8
5 Autores 9

1 SUMÁRIO EXECUTIVO

Uma nova vulnerabilidade crítica no **GNU/Linux**, descoberta por Simone Margaritelli, está gerando grande preocupação entre as principais distribuições Linux, como Ubuntu e Red Hat. Com uma pontuação de **9,9/10** na escala CVSS, esta falha representa um sério risco de segurança para milhões de sistemas globalmente.

2 INFORMAÇÕES SOBRE A VULNERABILIDADE

Há três semanas, Simone Margaritelli identificou uma vulnerabilidade RCE (Remote Code Execution) não autenticada que afeta todos os sistemas GNU/Linux e possivelmente outras plataformas. Essa falha permite que invasores remotos executem código arbitrário sem necessidade de autenticação, tornando-a extremamente perigosa. A ausência de uma correção funcional agrava ainda mais a situação.

Segundo Margaritelli, tanto a Canonical quanto a Red Hat confirmaram a gravidade da vulnerabilidade, que recebeu uma pontuação de 9,9/10 na escala CVSS. Isso indica um impacto devastador na segurança, com potencial para uso massivo por cibercriminosos se não for tratada rapidamente. Atualmente, não há CVE (Common Vulnerabilities and Exposures) atribuídos, embora Margaritelli acredite que pelo menos 3 ou 4 CVEs sejam necessários para cobrir diferentes aspectos da vulnerabilidade.

A falta de uma correção funcional gerou debates na comunidade de desenvolvedores, com alguns minimizando o impacto das vulnerabilidades. Margaritelli expressou sua frustração no Twitter, mencionando a resistência dos desenvolvedores em aceitar a falha no código subjacente. Apesar de seguir o protocolo de divulgação responsável, Margaritelli encontrou comportamento não cooperativo, levando-o a optar por uma divulgação completa da vulnerabilidade nas próximas semanas.

A vulnerabilidade foi classificada com uma pontuação CVSS v3.1 de 9,9/10, destacando seu extremo perigo. Os fatores que contribuíram para essa pontuação incluem:

- Vetor de Ataque (AV): Rede (N) — Exploração remota pela rede.
- Complexidade do Ataque (CA): Baixa (B) — Requer poucos pré-requisitos.
- Privilégios Necessários (PR): Nenhum (N) — Não requer privilégios de administrador.
- Interação do Usuário (IU): Nenhuma (N) — Não requer interação do usuário.
- Confidencialidade ©: Baixa (L) — Impacto moderado na privacidade.
- Integridade (I): Alta (H) — Compromete a integridade do sistema.
- Disponibilidade (A): Baixa (L) — Impacto moderado na disponibilidade do sistema.

Esses fatores combinados fazem desta uma das vulnerabilidades mais sérias no mundo GNU/Linux, especialmente preocupante para usuários corporativos e de data centers. Embora ainda não se saiba qual serviço específico é afetado, há especulações sobre o OpenSSH ou serviços de filtragem como Net Filter.

Simone Margaritelli, conhecido como evilsocket, é um renomado pesquisador de segurança cibernética, criador de ferramentas como o Bettercap, amplamente utilizado para ataques Man-in-the-Middle (MITM) e testes de penetração de rede. O Bettercap é valorizado por sua modularidade e flexibilidade, permitindo monitoramento e manipulação de tráfego em tempo real, análise de pacotes de rede e execução de ataques complexos. Mais detalhes sobre o Bettercap podem ser encontrados no site oficial do projeto.

Bettercap é uma ferramenta que oferece um conjunto abrangente de ferramentas de segurança de rede, permitindo a execução de ataques MITM, manipulação de tráfego e monitoramento de rede em tempo real. Criada inicialmente como uma alternativa moderna a ferramentas como Ettercap, Bettercap rapidamente se destacou como uma das ferramentas de segurança de rede mais potentes disponíveis atualmente.

Entre os principais recursos do Bettercap estão:

- **Modularidade**: Bettercap suporta diversos módulos que permitem aos usuários realizar diferentes tipos de ataques e análises, como monitoramento de tráfego HTTP, injeção de conteúdo e detecção de credenciais.
- **Suporte multiplataforma**: Bettercap pode ser executado em vários sistemas operacionais, incluindo GNU/Linux, Windows e macOS, tornando-o extremamente versátil.
- **Extensibilidade**: Os usuários podem criar seus próprios módulos e scripts para estender a funcionalidade do Bettercap, adaptando-o às suas necessidades específicas.

A popularidade do Bettercap se deve, em parte, à sua interface simples, mas poderosa, que permite até mesmo a usuários com habilidades básicas de segurança de rede realizarem testes complexos com relativa facilidade. Devido à sua versatilidade, Bettercap é utilizado não apenas em testes de segurança, mas também no treinamento de profissionais de segurança e em contextos educacionais em universidades.

3 RECOMENDAÇÕES

Mantenha o sistema atualizado

- Sempre aplique atualizações e patches de segurança para o sistema operacional e todos os softwares instalados.

Use senhas fortes e políticas de senha

- Implemente políticas de senha robustas, exigindo senhas complexas e alterando-as regularmente.

Configure um firewall

- Utilize ferramentas como iptables ou ufw para configurar regras de firewall que limitem o tráfego de rede apenas ao necessário.

Autenticação de dois fatores (2FA)

- Adicione uma camada extra de segurança configurando a autenticação de dois fatores para acessos críticos.

Limite o acesso ao servidor

- Restrinja o acesso SSH apenas a endereços IP confiáveis e desative o login root remoto.

Monitore o sistema

- Utilize ferramentas de monitoramento como Lynis ou AIDE para verificar a integridade do sistema e detectar atividades suspeitas.

Faça backups regulares

- Realize backups frequentes dos dados e armazene-os em locais seguros para garantir a recuperação em caso de incidentes

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Managedserver**

5 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH