ALERTA DE VULNERABILIDADE

Várias falhas de segurança encontradas no software de monitoramento de rede Nagios XI

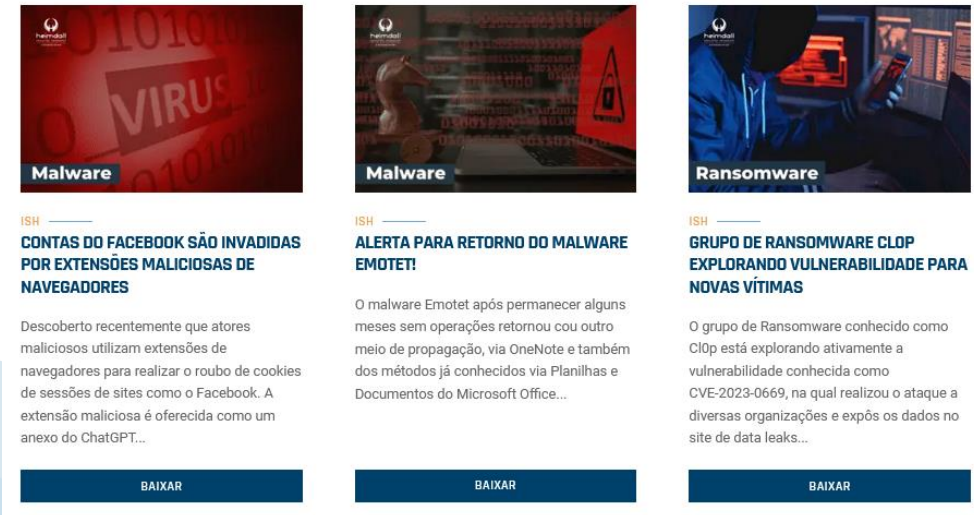
heimdall
security research
A DIVISION OF ISH

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso Twitter.

Heimdall Security Research

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 NAGIOS XI

O Nagios XI é uma popular ferramenta de monitoramento de rede usada por organizações para monitorar a integridade e o desempenho de seus ativos de TI, como servidores, dispositivos de rede e aplicativos. No entanto, como qualquer software, o Nagios XI não está imune a falhas de segurança.

Falhas de segurança em sistemas de monitoramento como o Nagios XI podem ter sérias implicações, pois essas ferramentas têm amplo acesso a informações críticas de sistemas e redes. Neste boletim de ameaças, exploraremos algumas recentes potenciais falhas de segurança que afetar o Nagios XI, bem como as implicações e melhores práticas para mitigar essas ameaças. É importante estar ciente dessas questões para garantir que o Nagios XI seja implementado e mantido de maneira segura em ambientes de TI.

2 VÁRIAS VULNERABILIDADES NO SOFTWARE

Foram descobertas várias falhas de segurança no software de monitoramento de rede **Nagios XI**, três das falhas de segurança identificadas (CVE-2023-40931, CVE-2023-40933 e CVE-2023-40934) possibilitam que usuários, com diferentes níveis de autorização, explorem vulnerabilidades de *SQL Injection* para acessar campos do banco de dados. A exploração dessas vulnerabilidades pode resultar na elevação de privilégios no produto e no acesso a informações confidenciais dos usuários, como hashes de senhas e tokens de API.

3 DETALHES DAS VULNERABILIDADES

Abaixo segue detalhes sobre as vulnerabilidades encontradas no software:

- **CVE-2023-40931** - Injeção de SQL no endpoint de reconhecimento de Banner
- **CVE-2023-40934** - Injeção de SQL no escalonamento de host/serviço no CCM
- **CVE-2023-40933** - Injeção de SQL nas configurações do banner de anúncio

Essas vulnerabilidades permitem que usuários, com vários níveis de privilégios, acessem campos de banco de dados via *SQL Injections*. Os dados obtidos dessas vulnerabilidades podem ser usados para aumentar ainda mais os privilégios no produto e obter dados confidenciais do usuário, como hashes de senha e tokens de API.

- **CVE-2023-40932** - Scripting entre sites no componente de logotipo personalizado

Esta vulnerabilidade está relacionada a uma falha de cross-site scripting (XSS) no componente Custom Logo que pode ser usado para ler dados confidenciais, incluindo senhas em texto não criptografado da página de login.

4 Conclusão

Em setembro de 2021, a empresa especializada em segurança cibernética industrial, identificou um total de onze vulnerabilidades no sistema Nagios. Essas vulnerabilidades representavam diversas ameaças, incluindo a possibilidade de falsificação de solicitações do lado do servidor (SSRF), falsificação de dados, escalonamento de privilégios em nível local, execução remota de código e vazamento de informações sensíveis.

No entanto, a empresa responsável pelo Nagios agiu prontamente para resolver essas vulnerabilidades. Em 11 de setembro de 2023, foi lançada a versão 5.11.2 do Nagios, que incluiu as correções necessárias para mitigar essas ameaças de segurança, com isso recomendamos fortemente a atualização do software Nagios XI.

5 RECOMENDAÇÕES

Recomendamos que a atualização do software Nagios XI para a versão **5.11.2** é de vital importância para garantir a segurança e o desempenho contínuo do sistema de monitoramento.

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- [thehackernews]
- [outpost24]

heimdall
security research
A DIVISION OF ISH