BOLETIM DE SEGURANÇA

Cisco lança correção para vulnerabilidade de command injection no Cisco IMC que permite elevação de privilégios

heimdall
security research
A DIVISION OF ISH

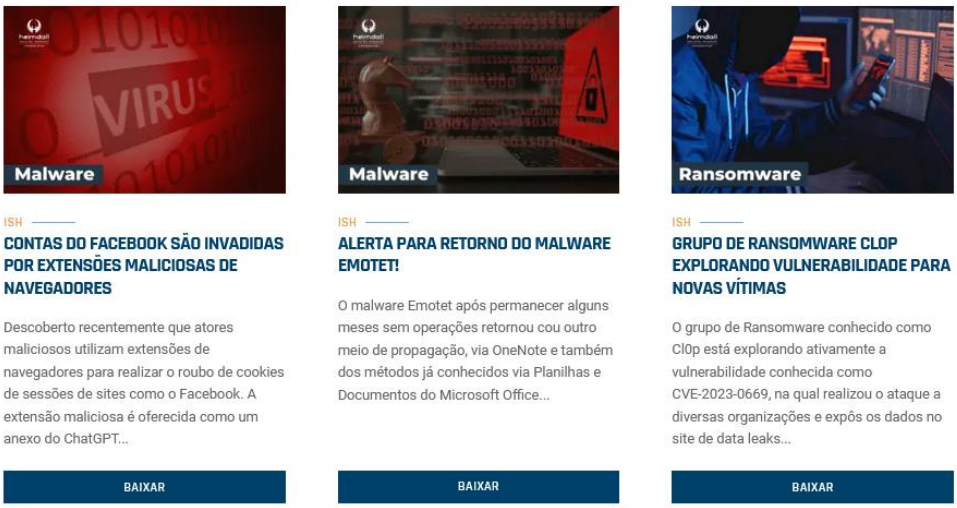
TLP: CLEAR

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

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 SUMÁRIO EXECUTIVO

A Cisco divulgou correções para uma vulnerabilidade CVE-2024-20295 de alta relevância no controlador de gerenciamento integrado (IMC), que, devido à existência de um código de exploração público, poderia possibilitar que atacantes obtivessem privilégios de root.

2 INFORMAÇÕES SOBRE A FALHA

O Cisco IMC, é um controlador de gerenciamento utilizado para a administração dos servidores UCS C-Series Rack e UCS S-Series Storage, opera através de interfaces diversas, como API XML, WebUI e CLI. Segundo a Cisco, uma falha na CLI do Cisco IMC poderia viabilizar que um atacante local com autenticação realizasse ataques de injeção de comando no sistema operacional, alcançando privilégios de root. A exploração da requer que o agressor possua privilégios de leitura ou superiores no equipamento comprometido. Esta falha de segurança decorre de uma inadequada validação de entradas de usuário, permitindo ataques de injeção de comando via CLI de baixa complexidade.

Os dispositivos afetados são:

- **Sistemas de computação de rede empresarial série 5000 (ENCS)**
- **Catalyst Série 8300 Edge uCPE**
- **Servidores Rack UCS Série C em modo autônomo**
- **Servidores UCS Série E**

3 RECOMENDAÇÕES

Para proteger-se contra essa vulnerabilidade, atualize os dispositivos afetados para a última versão de software disponibilizada pela Cisco. Monitore regularmente as comunicações da Cisco sobre atualizações de segurança e aplique-as prontamente. Considere a implementação de políticas de segurança rigorosas que restrinjam o acesso ao CLI apenas a usuários confiáveis e com a necessidade de uso comprovada.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Cisco**
- **Bleepingcomputer**

heimdall
security research
A DIVISION OF ISH