



# Apache

## BOLETIM DE SEGURANÇA

**CISA emite alerta sobre falha crítica no Apache  
HugeGraph-Server com exploração ativa**



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

## [Boletins de Segurança – Heimdall](#)



ISH

### CONTAS DO FACEBOOK SÃO INVADIDAS POR EXTENSÕES MALICIOSAS DE NAVEGADORES

Descoberto recentemente que atores maliciosos utilizam extensões de navegadores para realizar o roubo de cookies de sessões de sites como o Facebook. A extensão maliciosa é oferecida como um anexo do ChatGPT...

BAIXAR



ISH

### ALERTA PARA RETORNO DO MALWARE EMOTET!

O malware Emotet após permanecer alguns meses sem operações retornou com outro meio de propagação, via OneNote e também dos métodos já conhecidos via Planilhas e Documentos do Microsoft Office...

BAIXAR



ISH

### GRUPO DE RANSOMWARE CLOP EXPLORANDO VULNERABILIDADE PARA NOVAS VÍTIMAS

O grupo de Ransomware conhecido como Clop está explorando ativamente a vulnerabilidade conhecida como CVE-2023-0669, na qual realizou o ataque a diversas organizações e expôs os dados no site de data leaks...

BAIXAR

## SUMÁRIO

1	Sumário Executivo .....	5
2	Informações sobre as vulnerabilidades .....	6
3	Vulnerabilidades adicionadas ao KEV-CISA.....	7
4	Recomendações.....	8
5	Referências .....	9
6	Autores.....	10

## LISTA DE FIGURAS

Figura 1 – Vulnerabilidades no catálogo KEV-CISA. .... 7

## 1 SUMÁRIO EXECUTIVO

---

A Agência de Segurança Cibernética e Infraestrutura dos Estados Unidos (CISA) incluiu cinco novas vulnerabilidades no seu Catálogo de Vulnerabilidades Exploradas Conhecidas (KEV), entre elas uma falha [CVE-2024-27348](#) categorizada como crítica de execução remota de código (RCE) que afeta o **Apache HugeGraph-Server**. A vulnerabilidade está sendo explorada ativamente, o que levou a CISA a exigir que agências federais e organizações de infraestrutura crítica implementem as mitigações necessárias.

## 2 INFORMAÇÕES SOBRE AS VULNERABILIDADES

---

A vulnerabilidade, identificada como [CVE-2024-27348](#), recebeu uma classificação de risco crítico, trata-se de um problema relacionado ao controle de acesso inadequado que impacta as versões do HugeGraph-Server a partir da 1.0.0, exceto a 1.3.0. A falha foi corrigida pelo Apache no dia 22 de abril de 2024, com o lançamento da versão 1.3.0. Além da atualização para essa versão, os administradores foram orientados a utilizar o Java 11 e a ativar o sistema de autenticação.

O Apache HugeGraph-Server é o núcleo do projeto Apache HugeGraph, um banco de dados gráfico open-source, projetado para lidar com grandes volumes de dados gráficos, proporcionando alta escalabilidade e desempenho. Ele é amplamente utilizado em setores como telecomunicações, para detecção de fraudes e análise de redes, serviços financeiros, para controle de risco e análise de transações, e redes sociais, para análise de conexões e sistemas de recomendação. Dada a utilização do produto em ambientes corporativos críticos, a aplicação imediata das atualizações de segurança é imperativa para mitigar o risco.

Além dessa falha, a CISA adicionou outras quatro vulnerabilidades ao KEV:

- [CVE-2020-0618](#): Execução remota de código no Microsoft SQL Server Reporting Services.
- [CVE-2019-1069](#): Escalonamento de privilégios no Agendador de Tarefas do Microsoft Windows.
- [CVE-2022-21445](#): Execução remota de código no Oracle JDeveloper.
- [CVE-2020-14644](#): Execução remota de código no Oracle WebLogic Server.

Embora essas vulnerabilidades sejam antigas, sua inclusão no catálogo visa reforçar a documentação de falhas que foram comprovadamente exploradas em ataques passados.

### 3 VULNERABILIDADES ADICIONADAS AO KEV-CISA

A agência de segurança cibernética ([CISA](#)) adicionou as falhas ao seu Catálogo de Vulnerabilidades Exploradas Conhecidas ([KEV](#)), dizendo que tais vulnerabilidades são “vetores de ataque frequentes para atores cibernéticos maliciosos”.






<p>APACHE   HUGEGRAPH-SERVER</p> <p> <a href="#">CVE-2024-27348</a></p> <p><b>Apache HugeGraph-Server Improper Access Control Vulnerability:</b> <i>Apache HugeGraph-Server contains an improper access control vulnerability that could allow a remote attacker to execute arbitrary code.</i></p> <p>Known To Be Used in Ransomware Campaigns? <b>Unknown</b></p> <p><b>Action:</b> Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.</p> <ul style="list-style-type: none"> <li>■ <b>Date Added:</b> 2024-09-18</li> <li>■ <b>Due Date:</b> 2024-10-09</li> </ul>
<p>MICROSOFT   SQL SERVER</p> <p> <a href="#">CVE-2020-0618</a></p> <p><b>Microsoft SQL Server Reporting Services Remote Code Execution Vulnerability:</b> <i>Microsoft SQL Server Reporting Services contains a deserialization vulnerability when handling page requests incorrectly. An authenticated attacker can exploit this vulnerability to execute code in the context of the Report Server service account.</i></p> <p>Known To Be Used in Ransomware Campaigns? <b>Unknown</b></p> <p><b>Action:</b> Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.</p> <ul style="list-style-type: none"> <li>■ <b>Date Added:</b> 2024-09-18</li> <li>■ <b>Due Date:</b> 2024-10-09</li> </ul>
<p>MICROSOFT   TASK SCHEDULER</p> <p> <a href="#">CVE-2019-1069</a></p> <p><b>Microsoft Task Scheduler Privilege Escalation Vulnerability:</b> <i>A privilege escalation vulnerability exists in the way the Task Scheduler Service validates certain file operations.</i></p> <p>Known To Be Used in Ransomware Campaigns? <b>Known</b></p> <p><b>Action:</b> Apply updates per vendor instructions.</p> <ul style="list-style-type: none"> <li>■ <b>Date Added:</b> 2022-03-15</li> <li>■ <b>Due Date:</b> 2022-04-05</li> </ul>
<p>ORACLE   ADF FACES</p> <p> <a href="#">CVE-2022-21445</a></p> <p><b>Oracle ADF Faces Deserialization of Untrusted Data Vulnerability:</b> <i>Oracle ADF Faces library, included with Oracle JDeveloper Distribution, contains a deserialization of untrusted data vulnerability leading to unauthenticated remote code execution.</i></p> <p>Known To Be Used in Ransomware Campaigns? <b>Unknown</b></p> <p><b>Action:</b> Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.</p> <ul style="list-style-type: none"> <li>■ <b>Date Added:</b> 2024-09-18</li> <li>■ <b>Due Date:</b> 2024-10-09</li> </ul>
<p>ORACLE   WEBLOGIC SERVER</p> <p> <a href="#">CVE-2020-14644</a></p> <p><b>Oracle WebLogic Server Remote Code Execution Vulnerability:</b> <i>Oracle WebLogic Server, a product within the Fusion Middleware suite, contains a deserialization vulnerability. Unauthenticated attackers with network access via T3 or IIOP can exploit this vulnerability to achieve remote code execution.</i></p> <p>Known To Be Used in Ransomware Campaigns? <b>Unknown</b></p> <p><b>Action:</b> Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.</p> <ul style="list-style-type: none"> <li>■ <b>Date Added:</b> 2024-09-18</li> <li>■ <b>Due Date:</b> 2024-10-09</li> </ul>

Figura 1 – Vulnerabilidades no catálogo KEV-CISA.

## 4 RECOMENDAÇÕES

---

### **CVE-2024-27348**

- Vulnerabilidade relacionada a softwares de rede, requer atualização imediata para mitigar riscos de ataques remotos. Bloquear acessos não autorizados à rede para mitigar possíveis ataques de exploração de vulnerabilidades de rede.

### **CVE-2020-0618 e CVE-2022-21445**

- Vulnerabilidades em servidores SQL e Oracle, respectivamente, que podem ser corrigidas com atualizações críticas.
- Verificar as configurações de acesso ao Microsoft SQL Server. Auditar logs de servidores SQL para identificar tentativas de ataque ou atividades suspeitas de usuários não autorizados.

### **CVE-2019-1069**

- Monitorar comportamentos suspeitos associados à execução de comandos não autorizados em sistemas Windows. Educação sobre boas práticas em sistemas Windows, minimizando riscos associados a vulnerabilidades de execução de código.

### **CVE-2020-14644**

- Esses tipos de vulnerabilidades em servidores Oracle podem causar comprometimento crítico se não houver segmentação adequada.



## 5 REFERÊNCIAS

---

- Heimdall by ISH Tecnologia
- [CISA](#)
- [Bleepingcomputer](#)
- [NVD](#)

## 6 AUTORES

---

- Leonardo Oliveira Silva



heimdall  
security research

A DIVISION OF ISH