Prezado cliente,

A **Logical IT** alerta para a publicação do pacote de atualização de segurança da *Oracle* de Abril divulgado em *18 de Maio de 2020*. Neste pacote foram publicadas correções para atualizações de segurança em diversos produtos Oracle. Destacando-se uma vulnerabilidade crítica remotamente explorável no produto ***Oracle WebLogic Server*** do ***Oracle Fusion Middleware*** (componente: ***WLS Web Services***).

O produto ***WebLogic Server do Oracle Middleware Fusion*** é amplamente usado como um servidor de aplicativos de camada intermediária para executar aplicativos Web com a Tecnologia *Java*.

Esta vulnerabilidade é de fácil exploração e pode ser explorada remotamente.

Lista de Vulnerabilidades Críticas

- **CVE-2020-2798** - Oracle WebLogic Server Insecure Deserialization Vulnerability

Sistemas Afetados

- **Oracle Web Logic Server (Oracle Fusion Miidleware)** componente**: WLS Web Services** versões: "10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 e 12.2.1.4.0".

Vulnerabilidades Publicadas					
Identificação da Vulnerabilidades MITRE (CVE)	**Explorável Remoto?**	**Impacto**	**Divulgado Publicamente?**	**Exploração Disponível?**	**Pontuação de Severidade (CVSS)**
CVE-2020-2798	Sim	Remote Code Execution	Sim	Não	**7.2**

Serviço de Gestão de Vulnerabilidades		
Identificação da Vulnerabilidades MITRE (CVE)	**Nome da Assinatura**	**Data de Publicação**
CVE-2020-2798	**87416** - Oracle WebLogic Server Multiple Vulnerabilities (CPUAPR2020)	**15/04/2015**

MSS/SOC (Content Security)					
Identificação da Vulnerabilidades MITRE (CVE)	**Soluções: Trend Micro (Módulo: Virtual Patch)**				
	Deep Security	**Apex One**	**Vulnerability Protection (VP)**	**Tipping Point**	**Data da Última Atualização**
	Nome da Assinatura				
CVE-2020-2798	**1010242** - Oracle WebLogic Server	**N/A**	**N/A**	**37719**: TCP: Oracle WebLogic	**DS/VP 19/05/2020**

	Insecure Deserialization Vulnerability (CVE-2020-2798) Padrão da Assinatura (**Detect Only**)			Server T3 Protocol Java Deserialization Vulnerability Ação Padrão (**Block / Notify**)	**TP (Release) 05/05/2020**

Recomendação para solução definitiva

A Oracle publicou em seu informativo mensal a recomendação para atualização do seu produto que corrige em definitivo a vulnerabilidade no produto *Oracle Web Logic*.

Workarounds e Fatores de Mitigação

Recomenda-se sempre diminuir a exposição desnecessária de serviços, publicando as aplicações somente para os recursos e usuários necessários.
Adicionalmente caso não seja possível atualizar, recomenda-se utilizar uma solução com assinaturas de patches virtuais.

Como a LIT suporta nossos clientes para endereçar o risco destas ameaças no ambiente dos nossos clientes.

Nossos especialistas **coordenarão em paralelo com nossos clientes** um plano para implementação das ações de identificação, detecção e proteção planejadas para controlar o risco de potenciais explorações desta ameaça.

- **Identificação da Fragilidade (Gestão de Vulnerabilidades);**

Através do nosso serviço de Gestão de Vulnerabilidades agimos proativamente executando varreduras planejadas com os nossos clientes para identificações específicas para as fragilidades reportadas.

- **Detecção de Ameaças (SOC);**

O Nosso serviço do Centro de Operações de Segurança usa da base de Inteligência de Ameaças e Base de Conhecimento de comportamento para criar alertas personalizados para detectar e caçar explorações de ameaças, suportando agilidade na resposta e redução de impactos potenciais.

- **Proteção de Explorações (MSS);**

Nosso time de MSS trabalhará no planejamento e Implementação de Bloqueio das Ameaças **remotamente exploráveis** através das soluções com a tecnologia de **virtual patch** para as vulnerabilidades consideradas como remotamente exploráveis.

O Time da Logical IT está à disposição para mais esclarecimentos.

Informações adicionais (Ref.):

https://www.oracle.com/security-alerts/cpuapr2020.html

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-2798

https://nvd.nist.gov/vuln/detail/CVE-2020-2798

https://discussions.qualys.com/docs/DOC-7171-new-qid-for-vulnerabilities-in-oracle-weblogic-server

https://success.trendmicro.com/solution/TP000251935-Digital-Vaccine-9413