

4. Conhecendo Vulnerabilidades

Tipos de Vulnerabilidades

- Não existe ainda consenso sobre classificação e/ou taxonomia para vulnerabilidades
 - ➔ Por serviço afetado
 - ➔ Por gravidade
 - ➔ Por sistema operacional alvo
- Classificação por impacto potencial
 - ➔ Vulnerabilidades Críticas
 - ➔ Vazamento de informações
 - ➔ Negação de serviços
 - ➔ Falha em implementar melhores práticas

Vulnerabilidades críticas

- São os problemas de mais alta prioridade
- A sua exploração pode levar a execução de programas, escalada de privilégios, comprometimento do sistema, etc
- Critérios para classificar uma falha como crítica
 - ➔ Possibilidade de exploração remota
 - ➔ Exploração sem conta de usuário local
 - ➔ Permissão de acesso privilegiado
 - ➔ Exploração automática e confiável (para o atacante)
- Os Vermes exploram vulnerabilidades críticas

Vulnerabilidades - Suporte

- **Roubo de senhas** – Uso de senhas em branco, senhas previsíveis ou que não usam requisitos mínimos de complexidade. Deixar um Postit com a sua senha grudada no monitor é uma vulnerabilidade;
- **Configuração Incorreta** – Aplicativos executados com contas de Sistema Local, e usuários que possuem permissões acima do necessário;
- **Engenharia Social** – O Administrador pode alterar uma senha sem verificar a identidade da chamada;
- **Segurança fraca no Perímetro** – Serviços desnecessários, portas não seguras. Firewall e Roteadores usados incorretamente;
- **Transporte de Dados sem Criptografia** – Pacotes de autenticação usando protocolos de texto simples, dados importantes enviados em texto simples pela Internet.

Vulnerabilidades - Suporte

■ Senhas Default

→ A maioria dos equipamentos e softwares vem configurados com usuários e senhas default (padrão), documentados e bem conhecidos

→ Elas facilitam a instalação e configuração inicial

→ É muito comum os administradores esquecerem de alterar esses usuários e contas

→ Exemplos:

→ Cisco: conta: cisco, senha: cisco

→ SNMP: comunidade public

→ Windows: administrator



The screenshot shows a web page titled "Default Passwords" from <https://cirt.net/passwords>. The page lists "latest Passwords" for "515 vendors, 2067 passwords". It includes a search bar and links to @passdb on Twitter and Firefox Search. Below the list is a table of vendor names and their corresponding default password entries.

2Wire, Inc.	360 Systems	3COM
3M	Accelerated Networks	ACCTON
Acer	Actiontec	Adaptec
ADC Krentox	AdComplete.com	AddPac Technology
Adobe	ADT	Adtech

3. D-Link - DSL-504

User ID	(none)
Password	private
Level	Administrator

4. D-Link - hubs/switches

Method	Telnet
User ID	D-Link
Password	D-Link

Vulnerabilidades - Suporte

■ Senhas Default

Seguro | <https://cirt.net/passwords>



Default Passwords

Search Passwordss

522 vendors, 2083 passwords

[@passdb on Twitter](#) / [Firefox Search](#)



2Wire, Inc.	360 Systems	3COM
3M	Accelerated Networks	ACCTON
Acer	Actiontec	Adaptec
ADC Kentrox	AdComplete.com	AddPac Technology
Adobe	ADT	Adtech
Adtran	Advanced Integration	AIRAYA Corp
Airlink	AirLink Plus	Aironet
Airway	Aladdin	Alcatel
Alien Technology	Allied Telesyn	Allnet

Vulnerabilidades - Suporte

■ Senhas Default

1. Cisco - *Cisco IDS*

User ID	root
Password	attack
Level	Administrator
Doc	

2. Cisco - *CiscoWorks 2000*

User ID	guest
Password	(none)
Level	User
Doc	

3. Cisco - *CiscoWorks 2000*

User ID	admin
Password	cisco
Level	Administrator

5. Cisco - *IOS*

Version	2600 series
Method	Multi
Password	c
Doc	
Notes	but these are common misconfigurations

6. Cisco - *IOS*

Method	Multi
User ID	ripeop
Password	(none)
Doc	

7. Cisco - *IOS*

Method	Multi
User ID	cisco

Vulnerabilidades - Suporte

■ Senhas Default

1. Microsoft - SiteServer

Version	3.x
Method	HTTP
User ID	LDAP_Anonymous
Password	LdapPassword_1
Doc	

4. Microsoft - Windows NT

Method	Multi
User ID	Administrator
Password	(none)
Level	Administrator
Doc	

9. Microsoft - SQL Server 2000

Version	SP3
User ID	sa
Doc	

2. Microsoft - Windows NT

Method	Multi
User ID	(NULL)
Password	(none)
Level	User
Doc	

5. Microsoft - Windows NT

Method	Multi
User ID	Guest
Password	Guest
Level	User
Doc	

9. Microsoft - SQL Server 2000

Version	SP3
User ID	sa
Level	System Administrator
Doc	

3. Microsoft - Windows NT

Method	Multi

6. Microsoft - Windows NT

Method	Multi

11. Microsoft - Wireless Access Point/Router

Version	MN700
User ID	MSHOME
Password	MSHOME
Doc	

Vulnerabilidades - Suporte

■ Configurações erradas

→ A vida dos administradores de sistemas e de redes é dura

→ Eles sempre têm que fazer muita coisa e às pressas

→ Por inexperiência, displicênciia ou pressa, muitas vezes configurações erradas ficam ativas por muito tempo

→ Exemplo: FTP anônimo

→ Para permitir que um web designer um administrador configure um FTP “seguro” e esquece da conta padrão “anonymous”

→ Um atacante coletou durante 3 meses o arquivo de senhas de uma instituição financeira, antes que o problema fosse detectado

Vulnerabilidades - Suporte

■ Backdoors

- ➔ Geralmente são programas que escutam portas e possibilitam algum tipo de acesso
- ➔ Redes com administradores inexperientes facilmente têm pelo menos um sistema com backdoors conhecidos
 - ➔ Trojans: capturadores de teclado, mouse, senhas, área de desktop, relay para outros sistemas
- ➔ Geralmente são instalados por um atacante para ter novo acesso após um ataque bem sucedido
- ➔ Ou seja, um backdoor significa que a rede já foi atacada e vários ativos podem ter sido comprometidos

Vulnerabilidades - Suporte

■ Backdoors

- O método mais frequente de instalação, nesse sentido, envolve a **inclusão de arquivo remoto ou *remote file inclusion* (RFI)**, que explora vulnerabilidades em aplicações que executam *scripts* externos.
- Nesse caso, a função desses recursos legítimos é “enganada” e induzida a fazer o download de um *backdoor* a partir de uma fonte remota.

Portas mais usadas

Porta	Serviço
21	FTP (File Transport Protocol) - file storage and retrieval
22	SSH, SFTP - secure shell and SSH based FTP
23	Telnet - non-secure shell
25	SMTP (Simple Mail Transfer Protocol)
53	DNS (Domain Name System)
80	HTTP (HyperText Transfer Protocol) .
110	POP (Post Office Protocol) - mail retrieval protocol
123	NTP (Network Time Protocol)
143	IMAP (Internet Message Access Protocol)
156	SQL - relational database
161 162	SNMP (Simple Network Management Protocol)
179	BGP (Border Gateway Protocol)
389	LDAP (Lightweight Directory Access Protocol)
443	HTTPS - secure HTTP

Vulnerabilidades críticas

■ Relatório da Auditoria de uma Invasão

Ação Realizada	Pacote Inicial	HH:MM:SS
Varredura de portas	24	03:34:09
Procura por vulnerabilidade no servidor web utilizando o Nikto *	9928	03:34:19
Navega com o Mozilla Firefox 1.0.7 a procura de falhas de PHP	38.305	03:34:43
Explora falha PHP para acessar o conteúdo do /etc/passwd	38.497	03:34:55
Explora falha PHP, mas não consegue acessar o conteúdo do /etc/shadow	38.588	03:35:01
Explora falha PHP para acessar detalhes da configuração de rede	38.697	03:35:22
Explora falha PHP para acessar informações sobre a versão do sistema	38.807	03:35:33
Explora falha PHP para instalar uma backdoor temporária utilizando NETCAT **	38.928	03:35:49
Abre uma conexão com a backdoor instalada, a partir do segmento SYN	39040	03:36:18
Conexão aceita	39042	03:36:18

* <https://cirt.net/Nikto2>

** <https://www.varonis.com/pt-br/blog/netcat-commands>

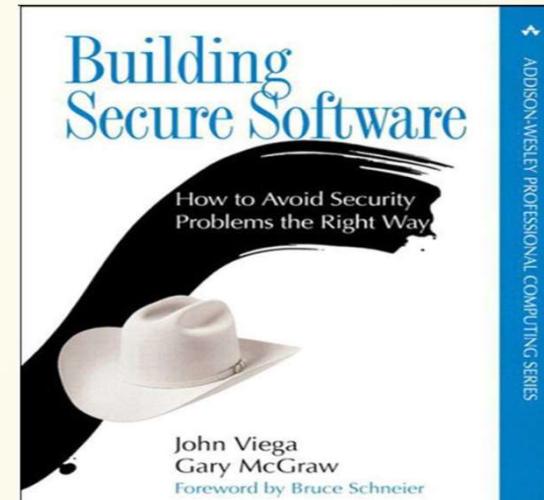
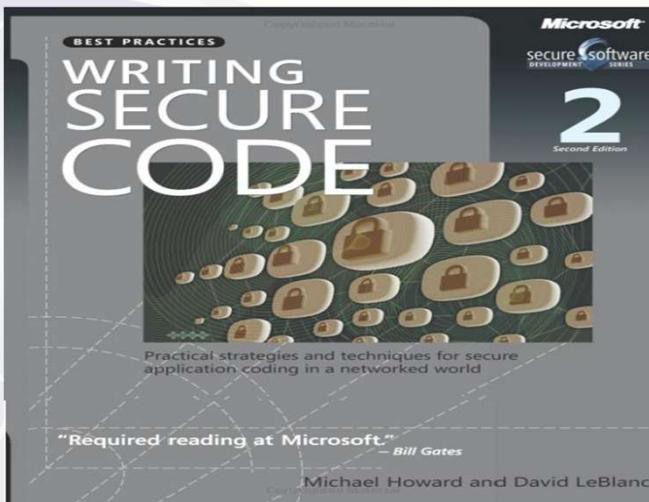
Vulnerabilidades críticas

■ Relatório da Auditoria de uma Invasão

Ação Realizada	Pacote Inicial	HH:MM:SS
Faz o download da figura <i>skull.jpg</i> na pasta <i>/tmp</i> , usando o comando wget	39129	03:38:11
Faz o download da página <i>skull.html</i> na pasta <i>/tmp</i> , usando o comando wget	39215	03:39:01
Faz o download do código fonte do exploit “ <i>km3.c</i> ” na pasta <i>/tmp</i> , usando o comando wget	39342	03:42:33
Compila o código fonte da exploit “ <i>km3.c</i> ” para o executável <i>owner_skull</i> , usando o comando gcc	39384	03:42:49
Executa o exploit <i>owner_skull -d</i>	39396	03:43:11
Comprova que se tornou o root por meio do comando <i>id</i>	39805	03:43:40
Retoma as tentativas de deface, usando o comando <i>cp</i>	39818	03:44:06
Instala uma backdoor definitiva com privilégios de root, dentro do <i>inetd.conf</i>	40300	03:50:12
Termina a conexão com a máquina invadida	40377	03:52:28

Vulnerabilidades Código

→Programação / Codificação



Vulnerabilidades críticas - Código

■ Erros de programação mais críticos

VERACODE

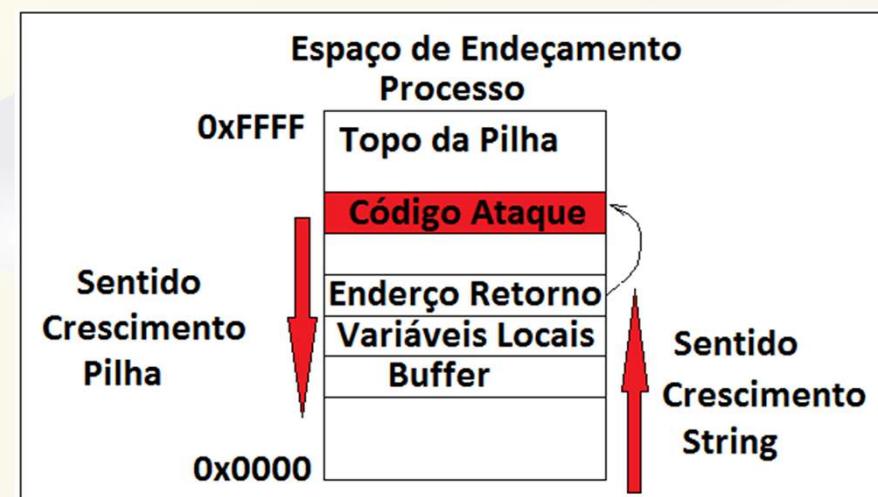
Buffer Overflow - Estouro de buffer ocorre quando há mais dados em um buffer do que ele pode manipular, fazendo com que os dados transbordem para o armazenamento adjacente;



Vulnerabilidades críticas - Código

■ Buffer Overflow

- O tipo mais famoso e explorado de vulnerabilidade crítica:
 - O programador não limita a quantidade de informação que pode ser escrita em uma determinada área de memória (string, array, etc);
 - O transbordo da memória ocorre quando o programa copia os dados de entrada para o buffer sem verificar o seu tamanho;
 - Metade das vulnerabilidades descobertas nos últimos anos são de buffer overflow (CERT).



Vulnerabilidades críticas - Código

■ Buffer Overflow Exemplos

Example Language: C

(Bad Code)

```
char last_name[20];
printf ("Enter your last name: ");
scanf ("%s", last_name);
```

Example Language: C

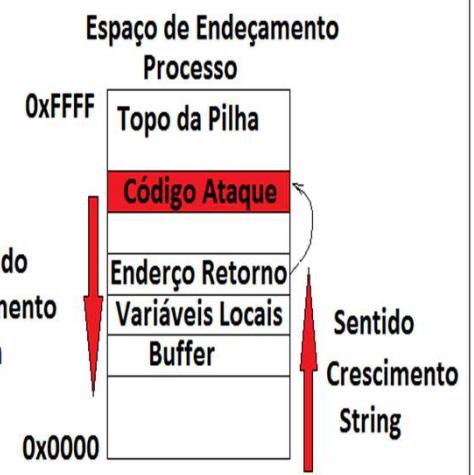
(Bad Code)

```
void manipulate_string(char* string){
    char buf[24];
    strcpy(buf, string);
    ...
}
```

Example Language: C

(Bad Code)

```
char buf[24];
printf("Please enter your name and press <Enter>\n");
gets(buf);
...
}
```



Vulnerabilidades críticas - Código

■ Buffer Overflow Exemplos

Example Languages: C and C++

(Bad Code)

```
...
struct hostent *clienthp;
char hostname[MAX_LEN];

// create server socket, bind to server address and listen on socket
...

// accept client connections and process requests
int count = 0;
for (count = 0; count < MAX_CONNECTIONS; count++) {

    int clientlen = sizeof(struct sockaddr_in);
    int clientsocket = accept(serversocket, (struct sockaddr *)&clientaddr, &clientlen);

    if (clientsocket >= 0) {
        clienthp = gethostbyaddr((char*) &clientaddr.sin_addr.s_addr, sizeof(clientaddr.sin_addr.s_addr), AF_INET);
        strcpy(hostname, clienthp->h_name);
        logOutput("Accepted client connection from host ", hostname);

        // process client request
        ...
        close(clientsocket);
    }
}
close(serversocket);
...
```

Vulnerabilidades críticas - Código

■ Erros de programação mais críticos

VERACODE

Vulnerabilidades de Programação / Software - Falhas ou fraquezas do sistema de software que podem ser exploradas por um atacante;

Injeção de CRLF - Os ataques de injeção de CRLF referem-se aos caracteres especiais "Carriage Return" e "Line Feed". As explorações ocorrem quando um invasor consegue injetar uma sequência CRLF em um fluxo HTTP;

Gerenciamento de credenciais - um ataque de gerenciamento de credenciais tenta violar os pares de nomes de usuário/senha e assumir o controle dessas contas;

Vulnerabilidades críticas - Código

■ Erros de programação mais críticos

VERACODE

Gerenciamento de credenciais - um ataque de gerenciamento de credenciais tenta violar os pares de nomes de usuário/senha e assumir o controle dessas contas;

INSECURE CODE

```
if ($_POST["submit"]){
    $username = $_POST[username];
    $sql = "SELECT COUNT(username) AS num FROM
account WHERE username = :username";
    $stmt = $pdo->prepare($sql);
    $stmt->bindValue(':username, $username);
    $stmt->execute();
    $row = $stmt->fetch(PDO::FETCH_ASSOC);
    if($row['num'] > 0){
        echo 'This user already exists, please choose a
new name.';
    }
}
```

Vulnerabilidades críticas - Código

■ Erros de programação mais críticos

VERACODE

Cross-Site Request Forgery - Cross-Site Request Forgery (CSRF) é um ataque malicioso que engana o navegador Web do usuário para executar ações indesejadas para que pareçam que um usuário autorizado está realizando essas ações;

Cross-Site Scripting - As vulnerabilidades XSS visam scripts incorporados em uma página que são executados no lado do cliente (no navegador da Web do usuário) ao invés de atacar o lado do servidor;

Directory Traversal - Travessia de Diretório é um tipo de exploração HTTP que é usado por invasores para obter acesso não autorizado a diretórios e arquivos restritos;

Vulnerabilidades críticas - Código

■ Travessia de Diretórios

- ➔ Problema comum encontrado em vários protocolos/aplicações que mapeiam pedidos dos usuários para caminhos de arquivos locais
- ➔ Exemplo: através de uma conta de FTP que remete ao /home/userX, o atacante consegue acessar outros diretórios e arquivos

Vulnerabilidades críticas - Código

■ Travessia de Diretórios

→ Vulnerabilidades descobertas

→ Apache

httpd-announce mailing list archives: August 2011

[Site index](#) · [List index](#)

Box list	
Dec 2016	5
Nov 2016	5
Oct 2016	5
Sep 2016	5
Aug 2016	1
Jul 2016	4
Jun 2016	5
May 2016	4
Apr 2016	2
Mar 2016	5
Feb 2016	4
Jan 2016	7
Dec 2015	5
Nov 2015	9
Oct 2015	6
Jul 2015	3
Jun 2015	2
May 2015	3
Apr 2015	1
Mar 2015	1
Sep 2014	1
Jul 2014	1

Message list	
Dirk-Willem van Gulik	Advisory: Range header DoS vulnerability Apache HTTPD 1.3/2.x \ (CVE-2011-3192\)
Dirk-Willem van Gulik	Advisory: Range header DoS vulnerability Apache HTTPD 1.3/2.x \ (CVE-2011-3192\)
Permalink (Message view)	
<p>From di...@apache.org (Dirk-Willem van Gulik) Subject Advisory: Range header DoS vulnerability Apache HTTPD 1.3/2.x \ (CVE-2011-3192\) Date Wed, 24 Aug 2011 16:16:39 GMT</p> <p>-----BEGIN PGP SIGNED MESSAGE----- Hash: SHA1 Apache HTTPD Security ADVISORY =====</p>	
<p>Title: Range header DoS vulnerability Apache HTTPD 1.3/2.x CVE: CVE-2011-3192: Date: 20110824 1600Z Product: Apache HTTPD Web Server Versions: Apache 1.3 all versions, Apache 2 all versions Description: =====</p> <p>A denial of service vulnerability has been found in the way the multiple overlapping ranges are handled by the Apache HTTPD server:</p> <p>http://seclists.org/fulldisclosure/2011/Aug/175</p> <p>An attack tool is circulating in the wild. Active use of this tools has</p>	

Vulnerabilidades críticas - Código

■ Erros de programação mais críticos



← → C Home 🔒 veracode.com

Contact Us Blog Community ▾ Login [Schedule a Demo](#) Q

VERACODE Products ▾ Solutions ▾ Developers ▾ Partners ▾ Resources ▾ About Us ▾

Veracode Obtains FedRAMP Authorization

Application Security Platform Now Available on FedRAMP Marketplace

 Learn More



Vulnerabilidades críticas - Código

■ Erros de programação mais críticos

VERACODE

VERACODE

Software Composition Analysis VULNERABILITY DATABASE | LOGIN

Vulnerability Database

language:java X 4,964,329 results

Search

Library

Vulnerability

Language/OS

Java

Ruby

JavaScript

Python

Objective-C

Swift

GO

PHP

C/C++

C#

OS

LIBRARY ARTIFACT SRCCLR-LID-1676482

firefox

Mozilla Firefox is an open-source web browser, designed for standards compliance, performance and portability.

Latest Version: 91.10.0--1.el8 Number of Vulnerabilities: 1124 Licenses vary by version OS (RPM)

LIBRARY ARTIFACT SRCCLR-LID-1676698

thunderbird

Mozilla Thunderbird is a standalone mail and newsgroup client.

Latest Version: 91.10.0--1.el8s Number of Vulnerabilities: 963 Licenses vary by version OS (RPM)

LIBRARY ARTIFACT SRCCLR-LID-1693923

java-1.6.0-ibm

Vulnerabilidades críticas - Código

■ Erros de programação mais críticos



VERACODE

Software Composition Analysis | VULNERABILITY DATABASE | LOGIN

Vulnerability Database

language:javascript

X 1,969,845 results

Search

Library

Vulnerability

Language/OS

JavaScript

Java

Ruby

Python

Objective-C

Swift

GO

PHP

C/C++

C#

OS

Vulnerability data is based on CVSS version 2 scores. To see results based on CVSS version 3 scores, adjust your [search criteria](#).

VULNERABILITY ARTIFACT SRCCLR-SID-6557

Man-in-the-Middle (MitM)

windows-seleniumjar-mirror is susceptible to man-in-the-middle (MitM) attacks. The attacker can download binary resources via HTTP, allowing MitM attacks. Since the attacker can replace the requested binary with its controlled binary if the attacker is on the network or positioned in between the user and the remote server, It can also lead to remote code execution (RCE).

9.3 CVE-2016-10670 1 library affected  Man-in-the-middle

VULNERABILITY ARTIFACT SRCCLR-SID-6491

Man-in-the-Middle (MitM)

grunt-webdriver-qunit is vulnerable to man-in-the-middle (MitM) attack. This is possible because it does not prevent downloading of executables via HTTP if the attacker is on the network or positioned in between the user and the remote server. Consequently, it may potentially cause remote code execution (RCE) by swapping out the requested binary with an attacker controlled binary.

9.3 CVE-2016-10606 1 library affected  Man-in-the-middle

VULNERABILITY ARTIFACT SRCCLR-SID-6476

Vulnerabilidades críticas - Código

■ Erros de programação mais críticos



SQL Injection - Injeção SQL é um tipo de vulnerabilidade de segurança de aplicação web em que um invasor é capaz de enviar um comando SQL de banco de dados, que é executado por uma aplicação web, expondo o banco de dados back-end;

Condição de corrida - Um ataque de condição de corrida acontece quando um sistema de computação projetado para lidar com tarefas em uma sequência específica é forçado a executar duas ou mais operações simultaneamente;

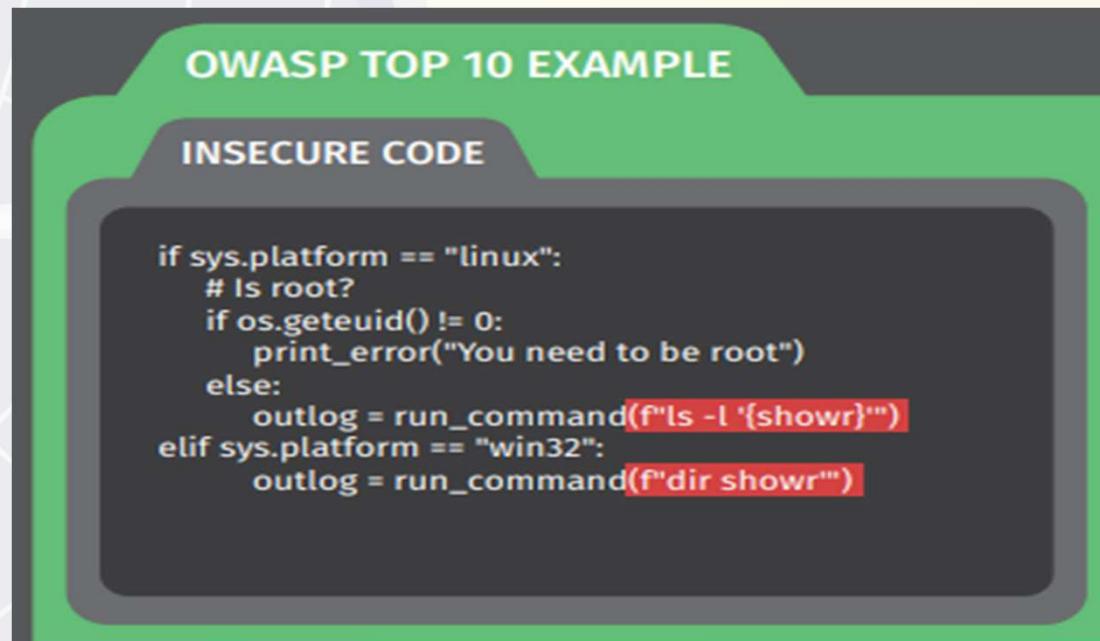
Injeção de comando do SO - A injeção de comando refere-se a uma classe de vulnerabilidades críticas de aplicativos que envolvem conteúdo gerado dinamicamente. Os invasores executam comandos arbitrários em um sistema operacional host usando um aplicativo vulnerável;

Vulnerabilidades críticas - Código

■ Erros de programação mais críticos



Injeção de comando do SO - A injeção de comando refere-se a uma classe de vulnerabilidades críticas de aplicativos que envolvem conteúdo gerado dinamicamente. Os invasores executam comandos arbitrários em um sistema operacional host usando um aplicativo vulnerável;



The card has a green header bar with the text "OWASP TOP 10 EXAMPLE" and a dark grey body. The title "INSECURE CODE" is centered above a code block.

```
if sys.platform == "linux":  
    # Is root?  
    if os.geteuid() != 0:  
        print_error("You need to be root")  
    else:  
        outlog = run_command(f"ls -l '{showr}'")  
elif sys.platform == "win32":  
    outlog = run_command(f"dir {showr}")
```

Vulnerabilidades críticas - Código

■ Erros de programação mais críticos

VERACODE

Código malicioso - código em qualquer parte de um sistema de software ou script que tenha a intenção de causar efeitos indesejados, violações de segurança ou danos a um sistema;

Injeção de LDAP - A injeção de LDAP (**Lightweight Directory Access Protocol**) é a técnica de exploração de aplicativos da Web que usam dados fornecidos pelo cliente em instruções LDAP sem primeiro remover caracteres potencialmente prejudiciais da solicitação.

Armazenamento criptográfico inseguro - O armazenamento criptográfico inseguro é uma vulnerabilidade comum que ocorre quando dados confidenciais não são armazenados com segurança de usuários internos;

Vulnerabilidades críticas - Código

■ Erros de programação mais críticos

VERACODE

Armazenamento criptográfico inseguro - O armazenamento criptográfico inseguro é uma vulnerabilidade comum que ocorre quando dados confidenciais não são armazenados com segurança de usuários internos;

INSECURE CODE

```
cipher.init(Algo.DES, ikey, vInit);
byte[] encryptedVal= new
byte[cipher.getOutputSize(input.length)];
int cipher_siz = cipher.update(input, 0,
input.length, encryptedVal, 0);
cipher_siz += cipher.doFinal(encryptedVal,
cipher_siz);
```

Vulnerabilidades críticas - Código

■ Formatação de strings

- ➔ Permite que um atacante passe como parâmetro especificadores de conversão (ex: "%d", "%s") e faça com que seja processados mais dados do que o programador considerou originalmente
- ➔ Permite que endereços de memória sejam sobrescritos e código malicioso seja executado
- ➔ O atacante precisa ter muito conhecimento, ou seja, precisa ser um “profissional”

Vulnerabilidades críticas - Código

■ Formatação de strings

→ Vulnerabilidades descobertas

→ Tripwire – Ferramenta Linux para Detecção Invasão

Uma vulnerabilidade foi encontrada em Tripwire IP360 VnE Vulnerability Manager 7.2.2/7.2.5 e classificada como crítico. Afectado é uma função desconhecida do componente *RPC Service*. A manipulação com uma entrada desconhecida leva a Fraca autenticação. Usar a CWE para declarar o problema leva à CWE-287. O resumo do CVE é:

The RPC service in Tripwire (formerly nCircle) IP360 VnE Manager 7.2.2 before 7.2.6 allows remote attackers to bypass authentication and (1) enumerate users, (2) reset passwords, or (3) manipulate IP filter restrictions via crafted "privileged commands."

O aconselhamento é partilhado para download em seclists.org.

A vulnerabilidade é identificada como [CVE-2015-6237](#). A atribuição do CVE aconteceu em 14/08/2015. O ataque pode ser feito a partir da rede. Não há detalhes técnicos disponíveis. A vulnerabilidade não é bem conhecida. Não há nenhuma exploração disponível.

Como 0 dia, o preço estimado do subsolo foi de cerca de \$0-\$5k.

A actualização para a versão 7.2.6 é capaz de abordar esta questão.

A vulnerabilidade está também documentada noutras bases de dados de vulnerabilidade: X-Force (106899).

Vulnerabilidades críticas - Código

- Formatação de strings
 - ➔ Vulnerabilidades descobertas
 - ➔ ISC DHCP FreeBSD

Synopsis

The remote FreeBSD host is missing one or more security-related updates.

Description

The ISC DHCP programs are vulnerable to several format string vulnerabilities which may allow a remote attacker to execute arbitrary code with the permissions of the DHCP programs, typically root for the DHCP server.

Solution

Update the affected packages.

Vulnerabilidades críticas - Código

■ Solaris rpc.rwalld (<https://vuldb.com/pt/?id.18393>)

Uma vulnerabilidade foi encontrada em Sun Solaris 2.6/7.0/8.0. Foi classificada como crítico. Afectado é a função `syslog` do componente *RPC Wall Daemon*. A manipulação com uma entrada desconhecida leva a Format String. A definição de CWE para a vulnerabilidade é CWE-134. Por CVE é registado:

Format string vulnerability in RPC wall daemon (rpc.rwalld) for Solaris 2.5.1 through 8 allows remote attackers to execute arbitrary code via format strings in a message that is not properly provided to the syslog function when the wall command cannot be executed.

O aconselhamento é partilhado para download em [cert.org](#).

A vulnerabilidade é identificada como CVE-2002-0573. O ataque pode ser iniciado a partir da rede. Os detalhes técnicos estão disponíveis. A vulnerabilidade não é bem conhecida. Além disso, há uma exploração disponível. Deve assumir-se que uma exploração custa actualmente cerca de USD \$0-\$5k.

É declarado como proof-of-concept. Esperamos que o dia 0 tenha valido aproximadamente \$25k-\$100k. O scanner de vulnerabilidade Nessus fornece um plugin com o ID 10950 (Solaris rpc.rwalld Remote Format String Arbitrary Code Execution), que ajuda a determinar a existência da falha num ambiente alvo. É atribuído à família *RPC*. O plugin está a funcionar no contexto do tipo *remote*.

Vulnerabilidades críticas - Código

- <https://www.whitesourcesoftware.com/vulnerability-database/>

WhiteSource

Product Solutions Pricing Company Resources Free Trial Log In

Top Vulnerabilities

* The table presents the most severe vulnerabilities published in the last 90 days

Vulnerability ID	Severity	Date Published	Action
CVE-2021-46250	10.0	15-02-2022	🔍 ✖
WS-2022-0048	10.0	22-01-2022	✖
CVE-2021-23594	10.0	10-01-2022	
WS-2021-0496	10.0	20-12-2021	✖ 🛡
WS-2021-0500	10.0	16-12-2021	✖
CVE-2021-44228	10.0	10-12-2021	✖ 🛡

Vulnerabilidades críticas - Código

■ <https://www.whitesourcesoftware.com/vulnerability-database/>

CVE-2021-46250

Good to know:



Date: February 15, 2022

An issue in SOA2Login::commented of ScratchOAuth2 before commit a91879bd58fa83b09283c0708a1864cdf067c64a allows attackers to authenticate as other users on downstream components that rely on ScratchOAuth2.

Language: PHP

Related Resources (3)

Url: <https://github.com/ScratchVerifier/ScratchOAuth2/commit/a91879bd58fa83b09283c0708a1864cd067c64a>

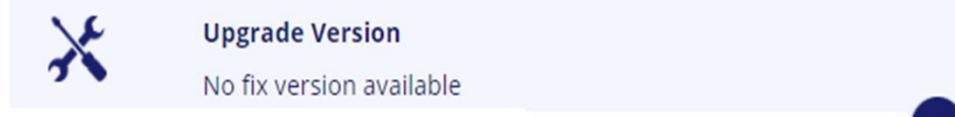
Url: <https://nvd.nist.gov/vuln/detail/CVE-2021-46250>

Url: <https://www.whitesourcesoftware.com/vulnerability-database/CVE-2021-46250>

Severity Score



Top Fix



Base Score:

Attack Vector (AV): NETWORK

Attack Complexity (AC): LOW

Privileges Required (PR): NONE

User Interaction (UI): NONE

Scope (S): CHANGED

Confidentiality (C): HIGH

Integrity (I): HIGH

Availability (A): HIGH

Explorações de Vulnerabilidades

■ <https://attack.mitre.org/techniques/T1190/>

Exemplos de procedimentos

EU IA	Nome	Descrição
G0007	APT28	O APT28 usou uma variedade de explorações públicas, incluindo CVE 2020-0688 e CVE 2020-17144, para obter execução no Microsoft Exchange vulnerável; eles também conduziram ataques de injeção de SQL contra sites externos. [10] [11]
G0016	APT29	APT29 explorou CVE-2019-19781 para Citrix, CVE-2019-11510 para VPNs Pulse Secure, CVE-2018-13379 para VPNs FortiGate e CVE-2019-9670 em software Zimbra para obter acesso. [12] [13]
G0087	APT39	APT39 usou injeção SQL para compromisso inicial. [14]
G0096	APT41	O APT41 explorou o CVE-2020-10189 contra o Zoho ManageEngine Desktop Central e o CVE-2019-19781 para comprometer Citrix Application Delivery Controllers (ADC) e dispositivos de gateway. [15]
G0001	Axioma	Axiom foi observado usando injeção de SQL para obter acesso a sistemas. [16] [17]
G0135	BackdoorDiplomacia	BackdoorDiplomacy explorou CVE-2020-5902, uma vulnerabilidade F5 BIP-IP, para eliminar um backdoor Linux. BackdoorDiplomacy também explorou servidores Plesk mal configurados. [18]

Explorações de Vulnerabilidades

■ <https://attack.mitre.org/techniques/T1190/>

APT28

APT28 é um grupo de ameaça que foi atribuído à unidade militar 26165 da Diretoria Principal de Inteligência do Estado-Maior General da Rússia (GRU) 85º Centro Principal de Serviços Especiais (GTsSS). [1] [2] Este grupo está ativo desde pelo menos 2004. [3] [4] [5] [6] [7] [8] [9] [10] [11] [12] [13]

O APT28 teria comprometido a campanha de Hillary Clinton, o Comité Nacional Democrata e o Comité de Campanha Democrata do Congresso em 2016, numa tentativa de interferir nas eleições presidenciais dos EUA. [5] Em 2018, os EUA indiciaram cinco oficiais da Unidade 26165 do GRU associados ao APT28 por operações cibernéticas (incluindo operações de acesso próximo) conduzidas entre 2014 e 2018 contra a Agência Mundial Antidopagem (WADA), a Agência Antidopagem dos EUA, uma instalação nuclear dos EUA, a Organização para a Proibição de Armas Químicas (OPAQ), o Laboratório Suíço de Produtos Químicos Spiez e outras organizações. [14] Alguns deles foram conduzidos com a assistência da Unidade GRU 74455, também conhecida como Equipe Sandworm .

Explorações de Vulnerabilidades

■ <https://attack.mitre.org/techniques/T1190/>

BackdoorDiplomacia

BackdoorDiplomacy é um grupo de ameaças de espionagem cibernética que está ativo pelo menos desde 2017. BackdoorDiplomacy tem como alvo Ministérios das Relações Exteriores e empresas de telecomunicações na África, Europa, Oriente Médio e Ásia. [1]

Técnicas Utilizadas

Camadas do Navegador ATT&CK ® ▾

Domínio	EU IA		Nome	Usar
Empreendimento	T1074	0,001	Preparação de dados : preparação de dados locais	BackdoorDiplomacy copiou arquivos de interesse para a lixeira da unidade principal. [1]
Empreendimento	T1190		Explorar aplicativos voltados ao público	BackdoorDiplomacy explorou CVE-2020-5902, uma vulnerabilidade F5 BIP-IP, para eliminar um backdoor Linux. BackdoorDiplomacy também explorou servidores Plesk mal configurados. [1]
Empreendimento	T1574	0,001	Fluxo de execução de sequestro : sequestro de ordem de pesquisa de DLL	BackdoorDiplomacy executou sequestro de ordem de pesquisa de DLL. [1]
Empreendimento	T1105		Transferência de ferramenta de entrada	BackdoorDiplomacy baixou arquivos e ferramentas adicionais em um host comprometido. [1]

Aspecto Financeiro Vulnerabilidades

Quanto Custa Corrigir uma Vulnerabilidade?

- Custo do Gerenciamento e planejamento da correção;
- Custo para encontrar o(s) erro(s);
- Custo da Correção em si;
- Custo de testar a solução;
- Custo de criar soluções adaptáveis em vários mercados;
- Custo de Disponibilização da solução no website da empresa;
- Custo de produção de documentação sobre o conserto;
- Custo com a perda de produtividade;
- Custo do desgaste da relação com os clientes;
- Custo de banda e hospedagem da solução em terceiros;
- Custo da perda de clientes.