Segurança em redes exemplos de exploits comuns e como lidar com elas

Giuliano Oliveira de Macedo

Segurança em redes

Giuliano Oliveira de Macedo

segurança em redes

Contextualização

Ataques

Heartbleed

RP Spoofing

Modelo de software TCP/IP

Pilha
Aplicação
Transporte
Rede
Enlace
Física

Segurança em redes

Giuliano Oliveira de Macedo

Importância de segurança em redes

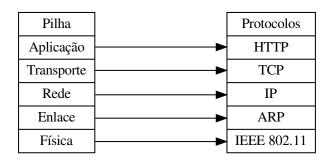
Contextualização

Ataque

Heartbleed

RP Spoofing

Modelo de software TCP/IP



Segurança em redes

Giuliano Oliveira de Macedo

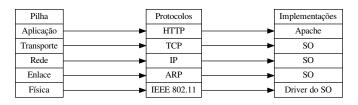
Importância de segurança em redes

Contextualização

Ataque

XSS Heartbleed

Modelo de software TCP/IP



Segurança em redes

Giuliano Oliveira de Macedo

Importância de segurança em redes

Contextualização

Ataque:

XSS Heartbleed

Contextualização

Segurança em redes

Giuliano Oliveira de Macedo

mportância de segurança em redes

Contextualização

Ataques

Heartbleed

CVE

Copy Results Download Results														
#	CVE ID	CWE ID #	of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1 🔼	E-2019-1020019	2 72		XSS	2019-07-29	2019-07-31	4.3	None	Remote	Medium	Not required	None	Partial	None
inveni	invenio-previewer before 1.0.0a12 allows XSS.													
2 <u>C\</u>	E-2019-1020018	3 20			2019-07-29	2019-10-09	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Discou	Discourse before 2.3.0 and 2.4.x before 2.4.0.beta3 lacks a confirmation screen when logging in via an email link.													
3 <u>C\</u>	E-2019-1020017	7 284			2019-07-29	2019-10-09	5.0	None	Remote	Low	Not required	None	Partial	None
Discou	Discourse before 2.3.0 and 2.4.x before 2.4.0 befa3 lacks a confirmation screen when logging in via a user-api OTP.													
4 🖸	E-2019-1020016	601			2019-07-29	2019-08-01	5.8	None	Remote	Medium	Not required	Partial	Partial	None
ASH-AIO before 2.0.0.3 allows an open redirect.														
5 <u>C\</u>	E-2019-1020019	5 20			2019-07-29	2019-08-05	5.0	None	Remote	Low	Not required	None	Partial	None
graphql-engine (aka Hasura GraphQL Engine) before 1.0.0-beta.3 mishandles the audience check while verifying JWT.														
6 <u>C\</u>	E-2019-1020014	4 415			2019-07-29	2019-08-19	2.1	None	Local	Low	Not required	Partial	None	None
docke	docker-credential-helpers before 0.6.3 has a double free in the List functions.													
7 🖸	E-2019-1020013	3 287			2019-07-29	2019-08-01	5.0	None	Remote	Low	Not required	Partial	None	None
parse-server before 3.6.0 allows account enumeration.														
8 🗥	E-2019-1020012	2 444			2019-07-29	2019-08-02	5.0	None	Remote	Low	Not required	None	None	Partial
parse-server before 3.4.1 allows DoS after any POST to a volatile class.														
9 <u>C\</u>	E-2019-1020011	20			2019-07-29	2019-10-09	6.5	None	Remote	Low	Single system	Partial	Partial	Partial

SmokeDetector intentionally does automatic deployments of updated copies of SmokeDetector without server operator authority.

Contextualização

- Exploits
 - Buffer overlfow
 - DoS
 - Execução de código
 - Corrupção de Memória
 - Sql Injection
 - XSS
 - Bypassing
 - Ganhar informações
 - Elevar previlégio
 - etc

Segurança em redes

Giuliano Oliveira de Macedo

Importância de segurança em redes

Contextualização

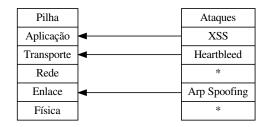
Ataques

XSS

ADD C (

Ataques

- XSS (Cross server scripting)
- ► Heartbleed (Buffer overflow no protocolo TLS)
- ARP Spoofing (Manipulação de servidores/clientes ARP com o fim de espionagem)



Segurança em redes

Giuliano Oliveira de Macedo

Importância de segurança em redes

Contextualização

Ataques

XSS Heartbleed ARP Spoofin



Giuliano Oliveira de Macedo

Importância de segurança em redes

Contextualização

Ataque

XSS

Heartbleed ARP Spoot

Heartbleed

Segurança em redes

Giuliano Oliveira de Macedo

Importância de segurança em redes

contextualização

Ataques

XSS

Heartbleed

ARP Spoofing

Segurança em redes

Giuliano Oliveira de Macedo

mportância de segurança em redes

contextualização

Ataques

YCC

Heartbleed
ARP Spoofing