مفاهیم امنیت

سپهر مقیسه

دکتر شهریاری

۹۸۳۱۱۰۳

پاییز ۱۴۰۱

.۱

تاثیر آسیبپذیری بروی صحت، محرمانگی، دسترس پذیری	پیچیدگی حمله	بسته یا برنامه حاوی آن آسیبپذیری	ورژن و نوع سیستم عامل تحت تاثیر	توضیح مختصر در مورد آسیبپذیری	شناسه آسیبپذیری
اختصاص حافظه بدون محدودیت- مصرف بی رویه منابع بدون دسترسی	۵,۵	crxFreeSubbandData	-	در برنامه libraw یک مشکل در حافظه است که در هنگام پردازش فایل های cr3 مشخص میشود	CVE-2020-35534
نوشتن داده خارج از ارایه و محدوده تعریف شده	۹,۸	Http client	-	در httpclient ممکن است یک نوشتن خارج از محدوده به دلیل داده های بدون مقدار صورت گیرد	CVE-2022-26437
نوشتن داده خارج از ارایه و محدوده تعریف شده	6.7	mailbox	-	در mailbox به دلیل چک نکردن کمبود حافظه میتواند نوشتن خارج از محدوده بکند	CVE-2022-26432
استفاده از عناصر و دستورات در قسمت کامند سیستم عامل	6.8	Ibm cics tx	11.1	در ibm cics هک کننده میتواند با دسترسی فیزیکی به دستگاه با کمک حمله برگشت و رفرش هک کند.	CVE-2022-33955

نوشتن خارج از محدوده	9.8	Omron cx	9.78	درomron cx با کمک نوشتن خارج از محدوده میتواند کد های خارجی را وارد کند	CVE-2022-3398

۲. الف) نصب انتی ویروس و پیشگیری چرا که ممکن است اگر الوده به ویروس شود بعضی او اطلاعات را پاک کند

ب)در بعضی اوقات که نیاز است یک سیستم خدماتی را ارائه دهد همیشه حمله عدم ارائه خدمات وجود دارد در این زمان باید این نوع حمله شناسایی شود تا از دسترس نرفتن سیستم جلوگیری شود

پ)در زمانی که هارد خراب شده، بازیابی اطلاعات بسیار مهم است چرا که به هرحال تمامی هارد ها بعد از مدتی میتوانند خراب شده و خطا دهند.

۳.بله میتواند. چرا که فرض کنید بین فرستنده و گیرنده یک فرد بدون اجازه در حال خواندن اطلاعات فرستنده است و در همین حین میتواند اطلاعات نا درست را به فرد گیرنده بفرستد.

.۴

	Attacks					
Service	Release of Message	Traffic Analysis	Masquerade	Replay	Modification of Message	Denial of Service
Peer Entity Authentication			Y			
Data Origin Authentication			Y			
Access Control			Y			
Confidentiality	Y					
Traffic-Flow Confidentiality		Y				
Data Integrity				Y	Y	
Non-Repudiation			Y			
Availability						Y

.۵

1.2	Release of message contents	Traffic analysis	Masquerade	Replay	Modification of messages	Denial of service
Encipherment	Y					
Digital signature			Y	Y	Y	
Access control	Y	Y	Y	Y		Y
Data integrity				Y	Y	
Authentication exchange	Y		Y	Y		Y
Traffic padding		Y				
Routing control	Y	Y				Y
Notarization			Y	Y	Y	

۶.

Ip spoofing به معنی ایجاد پکت ای پی و کپی از یک منبع ای پی دیگر است تا بتوان ip اصلی را مخفی کرد. سپس از این روش برای حمله ddos استفاده میکنند به این گونه که میتوان ip کپی شده را به گیرنده داد و در جواب پکت ارسالی را به جایی به غیر از فرستنده اصلی با ip اصلی، ارسال کنند. از این روش در زمانی که botnet وجود ندارد میتوان استفاده کرد که هم ای پی اصلی خود را مخفی کرده و هم بلاک کردن حمله کار سخت تری باشد.