

「CVSS」を使いこなすための勘所 ～ウェブサイト運営者になって～ <解答用紙>

独立行政法人 情報処理推進機構 (IPA)
セキュリティセンター
情報セキュリティ技術ラボラトリー

2010年12月6日公開

評価項目一覧

基本評価値 0.0 ~ 10.0	攻撃元区分	ローカル	隣接	ネット			
	攻撃条件複雑さ	高	中	低			
	認証要否	複数	単一	不要			
	機密性影響	なし	部分的	全面的			
	完全性影響	なし	部分的	全面的			
	可用性影響	なし	部分的	全面的			
現状評価値 0.0 ~ 10.0	攻撃可能性	未実証	実証可	攻撃可	容易	未評価	
	対策レベル	正式	暫定	非公式	未評価		
	情報信頼性	未確認	未確証	確認済	未評価		
環境評価値 0.0 ~ 10.0	二次的被害	なし	軽微	中程度	重大	壊滅的	未
	システム範囲	なし	小規模	中規模	大規模	未評価	
	セキュ要求(CIA)	低	中	高	未評価		

基本評価値 問題(1)

IPA Server OSにおけるサービス運用妨害 (DoS) の脆弱性

項目	選択肢・ポイント		
攻撃元区分 (AV Access Vector) <small>どこから攻撃可能であるか</small>	ローカル	隣接N/W	ネットワーク
攻撃条件複雑さ (AC Access Complexity) <small>攻撃する際に必要な条件の複雑さ</small>	高	中	低
攻撃前認証要否 (AU Authentication) <small>攻撃するために認証が必要であるか</small>	複数	単一	不要
機密性への影響 (C Confidentiality Impact) <small>機密情報が漏えいする可能性</small>	なし	部分的	全面的
完全性への影響 (I Integrity Impact) <small>情報が改ざんされる可能性</small>	なし	部分的	全面的
可用性への影響 (A Availability Impact) <small>業務が遅延・停止する可能性</small>	なし	部分的	全面的

値

基本評価値 問題(1)

IPA Server OSにおけるサービス運用妨害 (DoS) の脆弱性	
評価項目	理由 (メモ)
攻撃元区分 (AV)	
攻撃条件の複雑さ (AC)	
攻撃前の認証要否 (Au)	
機密性への影響 (C)	
完全性への影響 (I)	
可用性への影響 (A)	

基本評価値 問題(2)

IPA Vuln Web DBにおけるSQLインジェクションの脆弱性

項目	選択肢・ポイント		
攻撃元区分 (AV Access Vector) <small>どこから攻撃可能であるか</small>	ローカル	隣接N/W	ネットワーク
攻撃条件複雑さ (AC Access Complexity) <small>攻撃する際に必要な条件の複雑さ</small>	高	中	低
攻撃前認証要否 (AU Authentication) <small>攻撃するために認証が必要であるか</small>	複数	単一	不要
機密性への影響 (C Confidentiality Impact) <small>機密情報が漏えいする可能性</small>	なし	部分的	全面的
完全性への影響 (I Integrity Impact) <small>情報が改ざんされる可能性</small>	なし	部分的	全面的
可用性への影響 (A Availability Impact) <small>業務が遅延・停止する可能性</small>	なし	部分的	全面的

値

基本評価値 問題(2)

IPA Vuln Web DBにおけるSQLインジェクションの脆弱性	
評価項目	理由(メモ)
攻撃元区分 (AV)	
攻撃条件の複雑さ (AC)	
攻撃前の認証要否 (Au)	
機密性への影響 (C)	
完全性への影響 (I)	
可用性への影響 (A)	

基本評価値 問題(3)

IPA Vuln Web DBにおけるクロスサイト・スクリプティングの脆弱性

項目	選択肢・ポイント		
攻撃元区分 (AV Access Vector) どこから攻撃可能であるか	ローカル	隣接N/W	ネットワーク
攻撃条件複雑さ (AC Access Complexity) 攻撃する際に必要な条件の複雑さ	高	中	低
攻撃前認証要否 (AU Authentication) 攻撃するために認証が必要であるか	複数	単一	不要
機密性への影響 (C Confidentiality Impact) 機密情報が漏えいする可能性	なし	部分的	全面的
完全性への影響 (I Integrity Impact) 情報が改ざんされる可能性	なし	部分的	全面的
可用性への影響 (A Availability Impact) 業務が遅延・停止する可能性	なし	部分的	全面的

値

基本評価値 問題(3)

IPA Vuln Web DBにおけるクロスサイト・スクリプティングの脆弱性	
評価項目	理由(メモ)
攻撃元区分 (AV)	
攻撃条件の複雑さ (AC)	
攻撃前の認証要否 (Au)	
機密性への影響 (C)	
完全性への影響 (I)	
可用性への影響 (A)	

基本評価値 問題(4)

IPA Server OSにおけるバッファオーバーフローの脆弱性

項目	選択肢・ポイント		
攻撃元区分 (AV Access Vector) どこから攻撃可能であるか	ローカル	隣接N/W	ネットワーク
攻撃条件複雑さ (AC Access Complexity) 攻撃する際に必要な条件の複雑さ	高	中	低
攻撃前認証要否 (AU Authentication) 攻撃するために認証が必要であるか	複数	単一	不要
機密性への影響 (C Confidentiality Impact) 機密情報が漏えいする可能性	なし	部分的	全面的
完全性への影響 (I Integrity Impact) 情報が改ざんされる可能性	なし	部分的	全面的
可用性への影響 (A Availability Impact) 業務が遅延・停止する可能性	なし	部分的	全面的

値

基本評価値 問題(4)

IPA Server OSにおけるバッファオーバーフローの脆弱性	
評価項目	理由(メモ)
攻撃元区分 (AV)	
攻撃条件の複雑さ (AC)	
攻撃前の認証要否 (Au)	
機密性への影響 (C)	
完全性への影響 (I)	
可用性への影響 (A)	

基本評価値 問題(5)

解凍ソフトAにおけるバッファオーバーフローの脆弱性

項目	選択肢・ポイント		
攻撃元区分 (AV Access Vector) どこから攻撃可能であるか	ローカル	隣接N/W	ネットワーク
攻撃条件複雑さ (AC Access Complexity) 攻撃する際に必要な条件の複雑さ	高	中	低
攻撃前認証要否 (AU Authentication) 攻撃するために認証が必要であるか	複数	単一	不要
機密性への影響 (C Confidentiality Impact) 機密情報が漏えいする可能性	なし	部分的	全面的
完全性への影響 (I Integrity Impact) 情報が改ざんされる可能性	なし	部分的	全面的
可用性への影響 (A Availability Impact) 業務が遅延・停止する可能性	なし	部分的	全面的

値

基本評価値 問題(5)

解凍ソフトAにおけるバッファオーバーフローの脆弱性	
評価項目	理由(メモ)
攻撃元区分 (AV)	
攻撃条件の複雑さ (AC)	
攻撃前の認証要否 (Au)	
機密性への影響 (C)	
完全性への影響 (I)	
可用性への影響 (A)	