draft-li-sacm-light-weighted-vul-record-00

Li Jiang
China Mobile Research Institute
E-mail: lijiang@chinamobile.com

A new way to record vulnerability

1:
a vulnerability-->a detection-->a record
a vulnerability-->N detections-->N records(N>1)

2:
a vulnerability-->a detection-->a record
a vulnerability-->N detections-->a records(N>1)

{ non light-weighted vul record:

IP:A.B.C.D,

port:23,

service:telnet,

protocol:TCP,

vul_name:telnet weak password,

vul_detect_time:2020-10-11 10:20:30,

vul_detail:admin/123456

}

{Records from 2020-10-12 to 2020-10-16}

{

IP:A.B.C.D,

port:23,

service:telnet,

protocol:TCP,

vul_name:telnet weak password,

vul_detect_time:2020-10-17 10:20:30,

vul_detail:admin/123456

}

light-weighted vul record:

{

IP:A.B.C.D,

port:23,

service:telnet,

protocol:TCP,

vul_name:telnet weak password,

vul_status:0,

vul_det_time:2020-10-11 10:20:30,

vul_update_time:2020-10-17 10:20:30,

vul_fix_time:2020-10-17 10:20:30,

vul_detail:admin/123456

}

{

IP:A.B.C.D,

port:23,

service:telnet,

protocol:TCP,

vul_name:telnet weak password,

vul_status:0,

vul_det_time:2020-10-11 10:20:30,

vul_update_time:2020-10-18 10:20:30,

vul_fix_time:2020-10-18 10:20:30,

vul_detail:null

}

an example

A	B	C	D	E	F	G	H	I	J	K	L
IP	port	service	protocol	vul_name	vul_status	vul_det_time	vul_update_time	vul_fix_time	vul_detail		
218.	11211	memcache	TCP	memcache_unauth	0	2020/2/26 3:53:12	2020/8/27 20:56:45	2020/8/27 20:56:45	Unauthorized access		
117.1	11211	memcache	TCP	memcache_unauth	1	2020/2/26 11:18:26	2020/9/28 11:55:47		Unauthorized access		
218.20	11211	memcache	TCP	memcache_unauth	0	2020/2/26 12:19:44	2020/8/27 22:57:26	2020/8/27 22:57:26	Unauthorized access		
111.48	15000	memcached	TCP	memcache_unauth	0	2020/3/2 14:06:17	2020/8/27 17:23:40	2020/8/27 17:23:40	Unauthorized access		
218.20	12000	memcached	TCP	memcache_unauth	0	2020/3/3 2:42:40	2020/8/27 15:38:13	2020/8/27 15:38:13	Unauthorized access		
140.21	9900	memcached	TCP	memcache_unauth	0	2020/3/3 17:48:02	2020/9/10 11:24:48	2020/9/10 11:24:48	Unauthorized access		
183.218	12000	memcached	TCP	memcache_unauth	1	2020/3/4 0:08:36	2020/9/28 14:39:56		Unauthorized access		
211.141	20005	memcached	TCP	memcache_unauth	0	2020/3/4 0:13:40	2020/9/28 11:55:03	2020/9/28 11:55:03	Unauthorized access		
112.53	11211	memcache	TCP	memcache_unauth	0	2020/3/6 20:28:29	2020/8/28 2:12:59	2020/8/28 2:12:59	Unauthorized access		
112.53	11211	memcache	TCP	memcache_unauth	0	2020/3/6 20:28:38	2020/8/28 1:35:30	2020/8/28 1:35:30	Unauthorized access		
211.1	10010	memcached	TCP	memcache_unauth	0	2020/3/11 2:27:15	2020/9/28 11:38:14	2020/9/28 11:38:14	Unauthorized access		
112.1	8086	http	TCP	influxdb_unauth	1	2020/3/11 8:52:39	2020/10/9 21:16:11		influxdb vul exist:{"system": {"curre		
183.24	10004	http	TCP	influxdb_unauth	0	2020/3/11 8:53:24	2020/8/28 2:31:48	2020/8/28 2:31:48	influxdb vul exist:{"cmdline": ["/dat		
183.24	10009	http	TCP	influxdb_unauth	0	2020/3/11 8:53:24	2020/8/28 2:31:48	2020/8/28 2:31:48	influxdb vul exist:{"cmdline": ["/dat		
218.20	8086	http	TCP	influxdb_unauth	0	2020/3/11 8:53:24	2020/8/27 19:01:06	2020/8/27 19:01:06	influxdb vul exist:{"cmdline": ["/usr		
210.73	8086	http	TCP	influxdb_unauth	1	2020/3/11 8:53:25	2020/10/22 9:03:16		influxdb vul exist:{"system": {"curre		
43.247	8086	http	TCP	influxdb_unauth	0	2020/3/11 8:53:25	2020/8/27 18:56:48	2020/8/27 18:56:48	influxdb vul exist:{"system": {"curre		
117.15	8086	http	TCP	influxdb_unauth	0	2020/3/11 8:53:26	2020/8/28 0:06:51	2020/8/28 0:06:51	influxdb vul exist:{"system": {"curre		
117.13	8086	http	TCP	influxdb_unauth	1	2020/3/11 8:53:26	2020/9/28 15:35:21		influxdb vul exist:{"system": {"curre		
43.247.	8086	http	TCP	influxdb_unauth	0	2020/3/11 8:53:26	2020/9/28 15:36:15	2020/9/28 15:36:15	influxdb vul exist:{"system": {"curre		