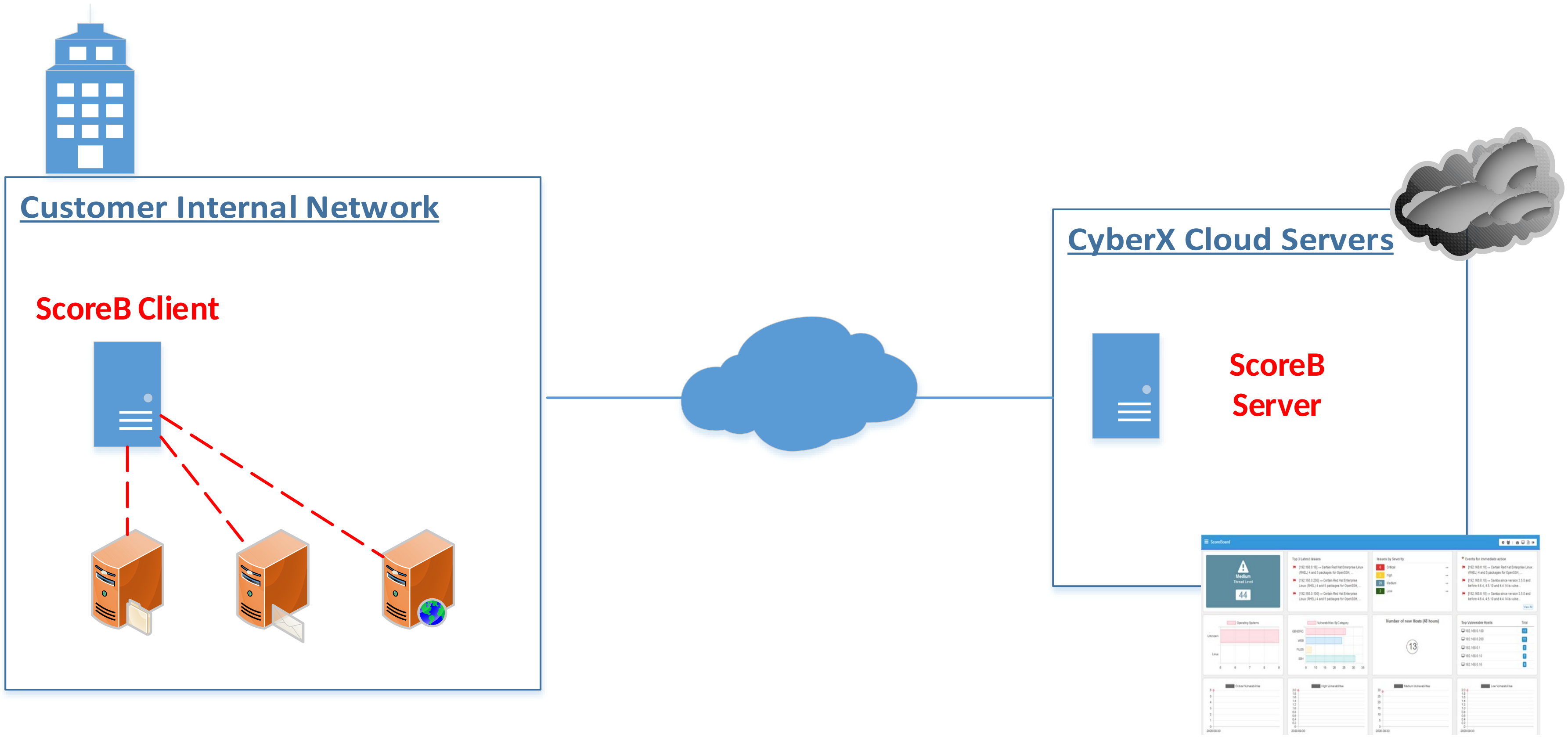
CyberX Security ScoreBoard

CyberX Networks

- What is it ?
  - A client/server application that automates the process of reconnaissance , scanning and enumeration for any given host or network.
  - It presents the results in a real-time dashboard with various graphs and statistics.
  - Runs its own Artificial Intelligence engine for events prioritization

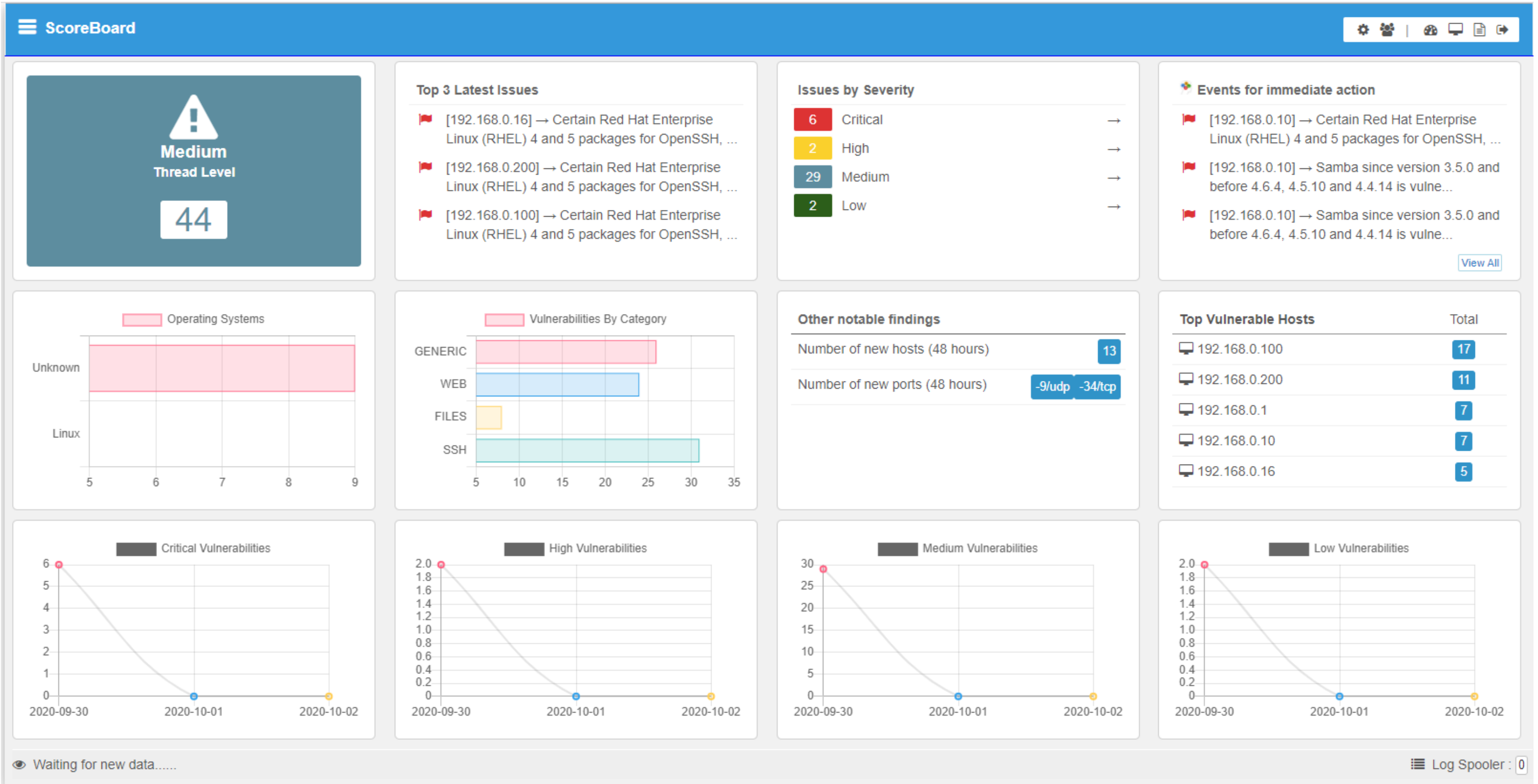
A hybrid model design that combines Internal and External automated penetration tests (blackbox).



- Built on top of well known Open Source Security Software and custom in-house penetration tools

- Supported by a team of Cyber Security Experts with more than 20 years of experience

A Real-Time dashboard, for all notable events



ScoreBoard

Medium
Thread Level
44

Top 3 Latest Issues

- [192.168.0.16] → Certain Red Hat Enterprise Linux (RHEL) 4 and 5 packages for OpenSSH, ...
- [192.168.0.200] → Certain Red Hat Enterprise Linux (RHEL) 4 and 5 packages for OpenSSH, ...
- [192.168.0.100] → Certain Red Hat Enterprise Linux (RHEL) 4 and 5 packages for OpenSSH, ...

Issues by Severity

6	Critical	→
2	High	→
29	Medium	→
2	Low	→

Events for immediate action

- [192.168.0.10] → Certain Red Hat Enterprise Linux (RHEL) 4 and 5 packages for OpenSSH, ...
- [192.168.0.10] → Samba since version 3.5.0 and before 4.6.4, 4.5.10 and 4.4.14 is vulne...
- [192.168.0.10] → Samba since version 3.5.0 and before 4.6.4, 4.5.10 and 4.4.14 is vulne...

View All

Other notable findings

Number of new hosts (48 hours)	13
Number of new ports (48 hours)	-9/udp -34/tcp

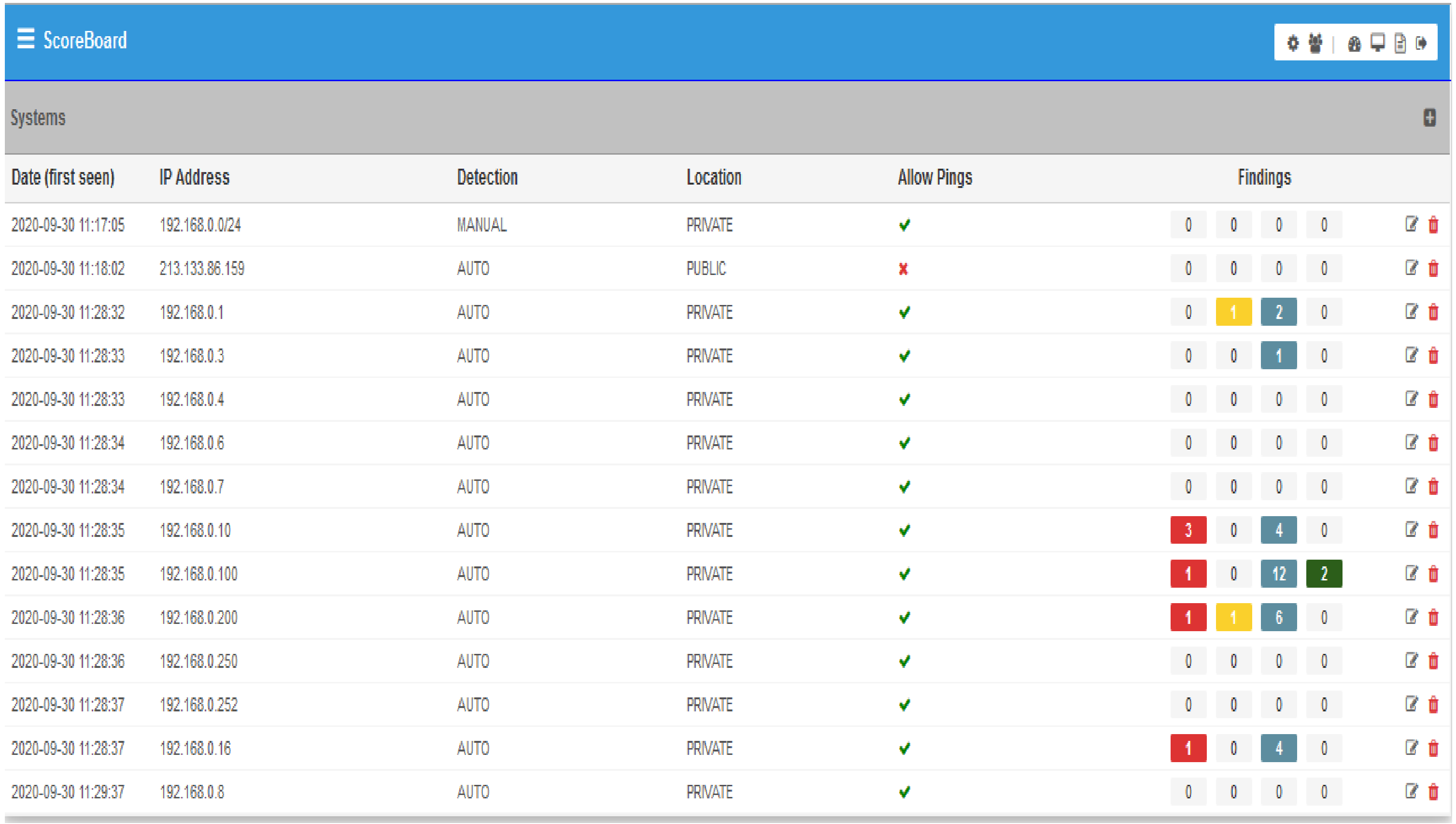
Top Vulnerable Hosts	Total
192.168.0.100	17
192.168.0.200	11
192.168.0.1	7
192.168.0.10	7
192.168.0.16	5

Waiting for new data......

Log Spooler : 0

CyberX
Networks

Automatic system discovery and categorization of findings based on CVE scoring & criticality



☰ ScoreBoard

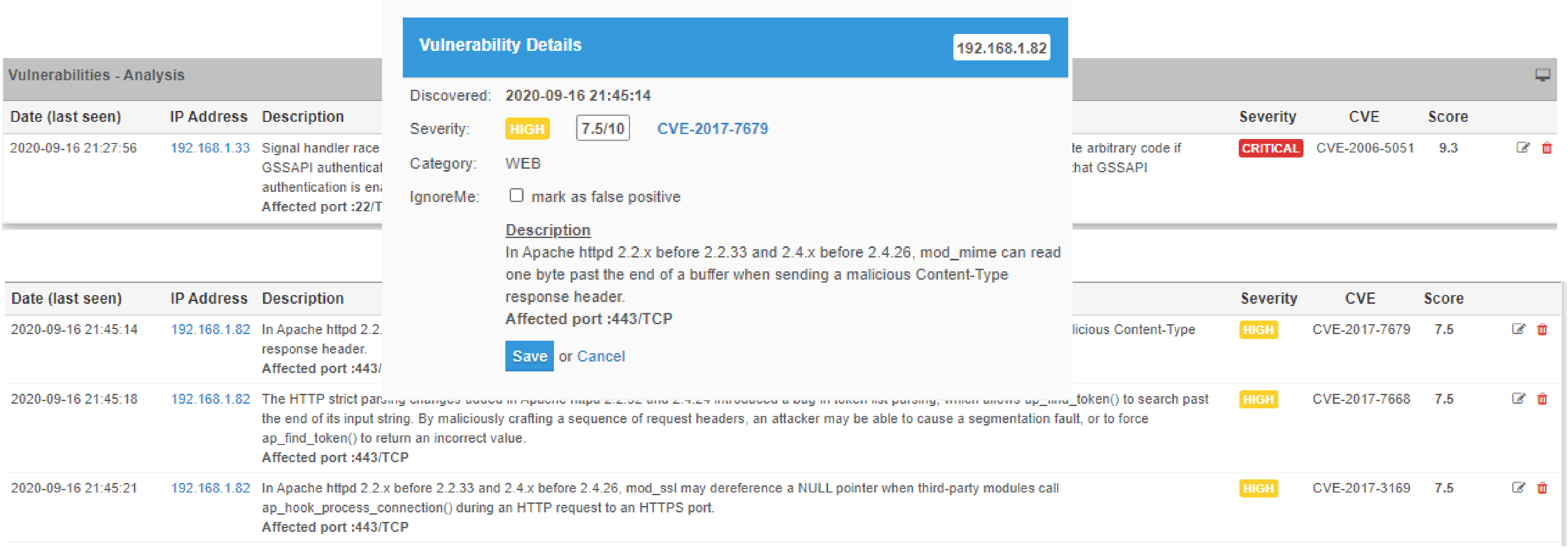
Systems

Date (first seen)	IP Address	Detection	Location	Allow Pings	Findings			
2020-09-30 11:17:05	192.168.0.0/24	MANUAL	PRIVATE	✓	0	0	0	0
2020-09-30 11:18:02	213.133.86.159	AUTO	PUBLIC	✗	0	0	0	0
2020-09-30 11:28:32	192.168.0.1	AUTO	PRIVATE	✓	0	1	2	0
2020-09-30 11:28:33	192.168.0.3	AUTO	PRIVATE	✓	0	0	1	0
2020-09-30 11:28:33	192.168.0.4	AUTO	PRIVATE	✓	0	0	0	0
2020-09-30 11:28:34	192.168.0.6	AUTO	PRIVATE	✓	0	0	0	0
2020-09-30 11:28:34	192.168.0.7	AUTO	PRIVATE	✓	0	0	0	0
2020-09-30 11:28:35	192.168.0.10	AUTO	PRIVATE	✓	3	0	4	0
2020-09-30 11:28:35	192.168.0.100	AUTO	PRIVATE	✓	1	0	12	2
2020-09-30 11:28:36	192.168.0.200	AUTO	PRIVATE	✓	1	1	6	0
2020-09-30 11:28:36	192.168.0.250	AUTO	PRIVATE	✓	0	0	0	0
2020-09-30 11:28:37	192.168.0.252	AUTO	PRIVATE	✓	0	0	0	0
2020-09-30 11:28:37	192.168.0.16	AUTO	PRIVATE	✓	1	0	4	0
2020-09-30 11:29:37	192.168.0.8	AUTO	PRIVATE	✓	0	0	0	0

CyberX
Networks

https://www.cyberxnetworks.com/

Full details and analysis of all findings. CVE number, score and on-line solutions also available.



Vulnerability Details 192.168.1.82

Discovered: 2020-09-16 21:45:14

Severity: HIGH 7.5/10 CVE-2017-7679

Category: WEB

IgnoreMe: □ mark as false positive

Description

In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

Affected port :443/TCP

Save or Cancel

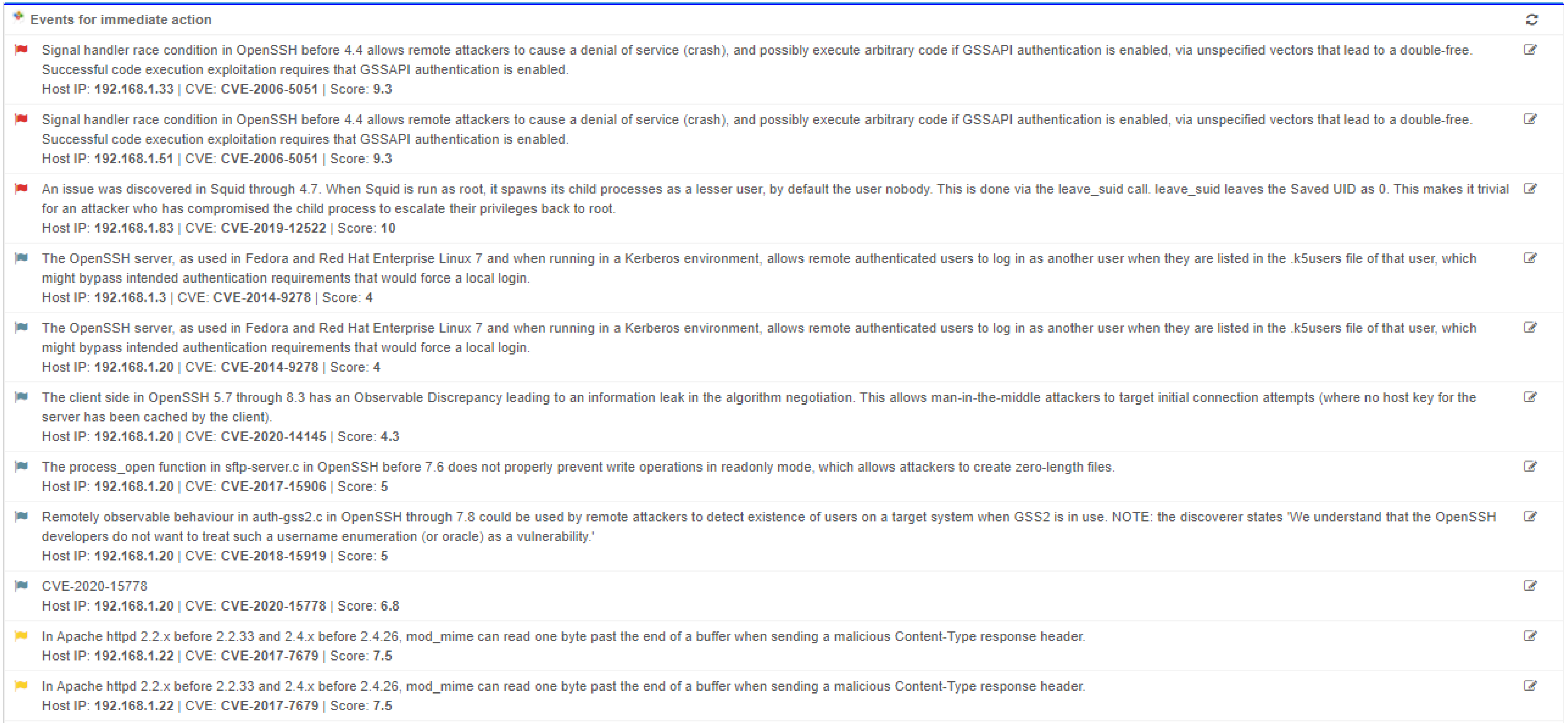
Vulnerabilities - Analysis

Date (last seen)	IP Address	Description	Severity	CVE	Score
2020-09-16 21:27:56	192.168.1.33	Signal handler race … te arbitrary code if GSSAPI authenticat … hat GSSAPI authentication is en… **Affected port :22/T**	CRITICAL	CVE-2006-5051	9.3

Date (last seen)	IP Address	Description	Severity	CVE	Score
2020-09-16 21:45:14	192.168.1.82	In Apache httpd 2.2. … licious Content-Type response header. **Affected port :443/**	HIGH	CVE-2017-7679	7.5
2020-09-16 21:45:18	192.168.1.82	The HTTP strict pars… …_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap_find_token() to return an incorrect value. **Affected port :443/TCP**	HIGH	CVE-2017-7668	7.5
2020-09-16 21:45:21	192.168.1.82	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port. **Affected port :443/TCP**	HIGH	CVE-2017-3169	7.5

CyberX Networks

Built-in Artificial Intelligence Engine for events prioritization based on system's classification



Events for immediate action

Signal handler race condition in OpenSSH before 4.4 allows remote attackers to cause a denial of service (crash), and possibly execute arbitrary code if GSSAPI authentication is enabled, via unspecified vectors that lead to a double-free. Successful code execution exploitation requires that GSSAPI authentication is enabled.
Host IP: **192.168.1.33** | CVE: **CVE-2006-5051** | Score: **9.3**

Signal handler race condition in OpenSSH before 4.4 allows remote attackers to cause a denial of service (crash), and possibly execute arbitrary code if GSSAPI authentication is enabled, via unspecified vectors that lead to a double-free. Successful code execution exploitation requires that GSSAPI authentication is enabled.
Host IP: **192.168.1.51** | CVE: **CVE-2006-5051** | Score: **9.3**

An issue was discovered in Squid through 4.7. When Squid is run as root, it spawns its child processes as a lesser user, by default the user nobody. This is done via the leave_suid call. leave_suid leaves the Saved UID as 0. This makes it trivial for an attacker who has compromised the child process to escalate their privileges back to root.
Host IP: **192.168.1.83** | CVE: **CVE-2019-12522** | Score: **10**

The OpenSSH server, as used in Fedora and Red Hat Enterprise Linux 7 and when running in a Kerberos environment, allows remote authenticated users to log in as another user when they are listed in the .k5users file of that user, which might bypass intended authentication requirements that would force a local login.
Host IP: **192.168.1.3** | CVE: **CVE-2014-9278** | Score: **4**

The OpenSSH server, as used in Fedora and Red Hat Enterprise Linux 7 and when running in a Kerberos environment, allows remote authenticated users to log in as another user when they are listed in the .k5users file of that user, which might bypass intended authentication requirements that would force a local login.
Host IP: **192.168.1.20** | CVE: **CVE-2014-9278** | Score: **4**

The client side in OpenSSH 5.7 through 8.3 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client).
Host IP: **192.168.1.20** | CVE: **CVE-2020-14145** | Score: **4.3**

The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.
Host IP: **192.168.1.20** | CVE: **CVE-2017-15906** | Score: **5**

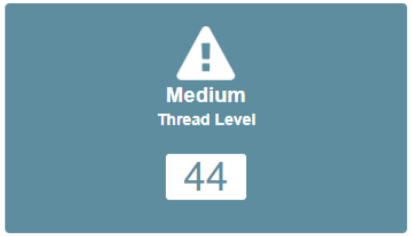
Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or oracle) as a vulnerability.'
Host IP: **192.168.1.20** | CVE: **CVE-2018-15919** | Score: **5**

CVE-2020-15778
Host IP: **192.168.1.20** | CVE: **CVE-2020-15778** | Score: **6.8**

In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.
Host IP: **192.168.1.22** | CVE: **CVE-2017-7679** | Score: **7.5**

In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.
Host IP: **192.168.1.22** | CVE: **CVE-2017-7679** | Score: **7.5**

Want even more ?



Medium

Thread Level

44

- Pre-built reports for the Management and IT experts
- Advanced algorithm for calculating the overall Thread Level
- Automatic updates of ALL system components (software , plugins etc)
- Virtual appliances for all know virtualization platforms.

Thank you

Any questions ?