

Errata - 3.2.2 Patch for match_ip_no_data

Coming in 3.3.0 is a new config item for matching devices called match_ip_no_data. This will be set to 'y' by default. This will be the last match item to be tested.

The idea behind match_ip_no_data is that if you are discovering a remote subnet and either have devices without management protocols, or devices that you don't have credentials for, you don't want duplicated devices.

By default the match_ip rule is set to 'n' because of DHCP. When you can a device on a remote subnet, the IP and DNS Hostname might be the only items that are returned. Neither of these are considered unique.

As a result, you often end up with duplicate devices.

match_ip_no_data hopes to address this.

If you have a result as above with precious little information, we will match on a device in the system table with the same IP, but only if it has not been audited (ie, it has an unknown or unclassified type and/or no serial number).

It's like a "match of last resort".

Hopefully this will prevent the duplicate devices from appearing.

Really though - you should have credentials for devices you are discovering 😊

This code (along with the new config item) will be included in 3.3.0.

To enable this (albeit without the config item to disable it), edit the file:

Linux

```
/usr/local/open-audit/code_igniter/application/models/m_devices.php
```

Windows

```
c:\xampp\open-audit\code_igniter\application\models\m_devices.php
```

And add the code below starting at line 1271.

It should come after the match_hostname section and before the line.

```
$temp = @(string)$details->id;
```

```

        # check IP Address in system table for a device with no other data
        if ((empty($match->match_ip_no_data) or strtolower($match->match_ip_no_data) == 'y') and empty($details->id) and !empty($details->ip) and filter_var($details->ip, FILTER_VALIDATE_IP)) {
            # Check the system table for an ip match on a device without a type or serial
            if (empty($details->id)) {
                $sql = "SELECT system.id FROM system WHERE system.ip = ? AND system.ip NOT LIKE '127%' AND
system.ip NOT LIKE '1::%' AND system.status != 'deleted' and (system.type = 'unknown' or system.type =
'unclassified') and system.serial = ''";
                $sql = $this->clean_sql($sql);
                $data = array(ip_address_to_db($details->ip));
                $query = $this->db->query($sql, $data);
                $row = $query->row();
                if (count($row) > 0) {
                    $details->id = $row->id;
                    $log->system_id = $details->id;
                    $message = new stdClass();
                    $message->message = 'HIT on IP Address No Data (system table).';
                    $message->command_status = 'success';
                    $message->command_output = 'IP: ' . $details->ip . ', SystemID : ' . $details->id;
                    $log_message[] = $message;
                    foreach ($log_message as $message) {
                        $log->message = $message->message;
                        $log->command_status = $message->command_status;
                        $log->command_output = $message->command_output;
                        discovery_log($log);
                    }
                    $message->command_output = '';
                    return $details->id;
                }
            }
            $message = new stdClass();
            $message->message = 'MISS on IP Address No Data.';
            $message->command_status = 'notice';
            $message->command_output = 'IP: ' . $details->ip;
            $log_message[] = $message;
        } else {
            if (strtolower($match->match_ip) != 'y') {
                $message = new stdClass();
                $message->message = 'Not running match_ip_no_data, matching rule set to: ' . $match->match_ip
                . ' .';
                $message->command_status = 'notice';
                $message->command_output = '';
                $log_message[] = $message;
            } else if (!empty($details->id)) {
                $message = new stdClass();
                $message->message = 'Not running match_ip_no_data, device id already set';
                $message->command_status = 'notice';
                $message->command_output = '';
                $log_message[] = $message;
            } else if (empty($details->ip)) {
                $message = new stdClass();
                $message->message = 'Not running match_ip_no_data, ip not set.';
                $message->command_status = 'notice';
                $message->command_output = '';
                $log_message[] = $message;
            } else {
                $message = new stdClass();
                $message->message = 'Not running match_ip_no_data.';
                $message->command_status = 'notice';
                $message->command_output = '';
                $log_message[] = $message;
            }
        }
    }
}

```