CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the organisation specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the organisation or addresser, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Scan Date: 1/18/2018
Table of Contents

1 - Summary
2 - Details
   2.1 - Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)
   2.2 - Lighttpd Multiple vulnerabilities
   2.3 - BlackIce DoS (ping flood)
   2.4 - CERN httpd CGI name heap overflow
   2.5 - http TRACE XSS attack
   2.6 - KF Web Server /%00 bug
   2.7 - DCE/RPC and MSRPC Services Enumeration Reporting
   2.8 - Jenkins 2.93 XSS Vulnerability (Windows)
1 - Summary

This report gives details on hosts that were tested and issues that were found during the Internal Vulnerability Scan. The findings are grouped by category.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCE/RPC and MSRPC Services Enumeration Reporting</td>
<td>61</td>
</tr>
<tr>
<td>Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)</td>
<td>7</td>
</tr>
<tr>
<td>CERN httpd CGI name heap overflow</td>
<td>3</td>
</tr>
<tr>
<td>KF Web Server /%00 bug</td>
<td>2</td>
</tr>
<tr>
<td>BlackIce DoS (ping flood)</td>
<td>2</td>
</tr>
<tr>
<td>Jenkins 2.93 XSS Vulnerability (Windows)</td>
<td>1</td>
</tr>
<tr>
<td>Lighttpd Multiple vulnerabilities</td>
<td>1</td>
</tr>
<tr>
<td>http TRACE XSS attack</td>
<td>1</td>
</tr>
</tbody>
</table>
2 - Scan Details

This section details the issues discovered in order of severity. For each issue, the affected nodes are also listed.

![Issues by Severity](image)

### 2.1 - Microsoft Windows SMB Server Multiple Vulnerabilities - Remote (4013389)

**High**: (CVSS: 9.3)  
OID: 1.3.6.1.4.1.25623.1.0.810676

**Summary**
This host is missing a critical security update according to Microsoft Bulletin MS17-010.

**Affected Nodes**
10.0.8.27, 10.0.8.39, 10.0.8.37, 10.0.8.70, 10.0.8.102, 10.0.8.104, 10.0.9.41

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**
Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server. Impact Level: System

**Solution**
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/MS17-010

**Vulnerability Insight**
Multiple flaws exist due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.

**Vulnerability Detection Method**
Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulnerability.

**Details:** Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389) (OID: 1.3.6.1.4.1.25623.1.0.810676) Version used: $Revision: 7543$

**References**

### 2.2 - Lighttpd Multiple vulnerabilities

**High**: (CVSS: 7.5)  
OID: 1.3.6.1.4.1.25623.1.0.802072

**Summary**
This host is running Lighttpd and is prone to multiple vulnerabilities

**Affected Nodes**
### 10.0.8.169

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

<table>
<thead>
<tr>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Successful exploitation will allow remote attackers to execute arbitrary SQL commands and read arbitrary files via hostname. Impact Level: System/Application</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade to 1.4.35 or higher, For updates refer to <a href="http://www.lighttpd.net/download">http://www.lighttpd.net/download</a></td>
</tr>
</tbody>
</table>

**Vulnerability Insight**
- `mod_mysql_vhost` module not properly sanitizing user supplied input passed via the hostname.
- `mod_evhost` and `mod_simple_vhost` modules not properly sanitizing user supplied input via the hostname.

**Vulnerability Detection Method**
Send a crafted HTTP GET request and check whether it responds with error message. Details: Lighttpd Multiple vulnerabilities (OID: 1.3.6.1.4.1.25623.1.0.802072) Version used: $Revision: 7577$

**References**

---

### 2.3 - BlackIce DoS (ping flood)

**Summary**
It was possible to crash the remote machine by flooding it with 10 KB ping packets.

**Affected Nodes**
10.0.8.2, 10.0.9.199

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**
A cracker may use this attack to make this host crash continuously, preventing you from working properly.

**Solution**
Upgrade your BlackIce software or remove it.

**Vulnerability Detection Method**
Details: BlackIce DoS (ping flood) (OID: 1.3.6.1.4.1.25623.1.0.10927) Version used: $Revision: 6315$

---

### 2.4 - CERN httpd CGI name heap overflow

**Summary**
It was possible to kill the remote web server by requesting GET /cgi-bin/AAAA[...]/A HTTP/1.0 This is known to trigger a heap overflow in some servers like CERN HTTPD.

**Affected Nodes**
10.0.8.1, 10.0.8.9, 10.0.8.4

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**
A cracker may use this flaw to disrupt your server. It *might also be exploitable to run malicious code on the machine.*

**Solution**
Ask your vendor for a patch or move to another server

**Vulnerability Detection Method**
2.5 - http TRACE XSS attack

Summary
Debugging functions are enabled on the remote HTTP server. The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections. It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracking, when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Affected Nodes
10.0.8.12

Vulnerability Detection Result
Solution: Add the following lines for each virtual host in your configuration file:

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]
```

See also http://httpd.apache.org/docs/current/de/mod/core.html#traceenable

Solution
Disable these methods.

Vulnerability Detection Method
Details: http TRACE XSS attack (OID: 1.3.6.1.4.1.25623.1.0.11213) Version used: $Revision: 6063 $

References
http://www.kb.cert.org/vuls/id/867593

2.6 - KF Web Server /%00 bug

Summary
Requesting a URL with '/%00' appended to it makes some versions of KF Web Server to dump the listing of the directory, thus showing potentially sensitive files.

Affected Nodes
10.0.8.2, 10.0.9.199

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution
upgrade to the latest version of KF Web Server

Vulnerability Detection Method
Details: KF Web Server /%00 bug (OID: 1.3.6.1.4.1.25623.1.0.11166) Version used: $Revision: 8023 $

2.7 - DCE/RPC and MSRPC Services Enumeration Reporting

Summary
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

Affected Nodes
10.0.1.9(DC), 10.0.1.4, 10.0.1.5(VPNGW9), 10.0.1.6(ISA1), 10.0.1.15(UTIL12), 10.0.1.16(DEVNFS), 10.0.1.21(RGATEWAY), 10.0.1.23, 10.0.1.41(FILE2012-1), 10.0.1.69(STORE01), 10.0.1.81(FINANCE), 10.0.1.100(HV00), 10.0.1.104(HV44), 10.0.1.120(HV42), 10.0.1.121(HV02), 10.0.8.0(MWEST-PC),
Vulnerability Detection Result

Here is the list of DCE/RPC or MSRPC services running on this host via the TCP protocol: Port: 49152/tcp
UIID: d95afe70-a6d5-4259-822e-2c84da1dbd0, version 1  Endpoint: ncacn_ip_tcp:10.0.1.3[49152] Port: 49153/tcp
2.8 - Jenkins 2.93 XSS Vulnerability (Windows)

Summary
Jenkins through 2.93 is prone to an XSS vulnerability.

Affected Nodes
10.0.9.99

Vulnerability Detection Result
Installed version: 2.89.2 Fixed version: NoneAvailable

Impact
Successful exploitation would allow an authenticated attacker to expose other users malicious code.

Solution
No solution as of 7th December 2017. This will be updated once a solution is available.

Vulnerability Insight
An authenticated attacker can use a crafted tool name in a job configuration form to conduct XSS attacks.

Vulnerability Detection Method
The script checks if the vulnerable version is present on the target host. Details: Jenkins 2.93 XSS Vulnerability (Windows) (OID: 1.3.6.1.4.1.25623.1.0.113064) Version used: $Revision: 8028 $

Product Detection Result
Product: cpe:/a:cloudbees:jenkins:2.89.2 Method: Jenkins CI Detection (OID: 1.3.6.1.4.1.25623.1.0.111001)

References
https://jenkins.io/changelog/