README.md

Usermin

Vulnerabilities for usermin 1.850 and prior.

Code Execution 1 - CVE-2022-35132

Type: Authenticated code execution

A authenticated user can execute commands using the GPG module. This is useful if the shell module has been restricted for that user.

Vulnerability:

`import.cgi` line 24 executes unsanitized user input.

```
$out = `$gpgpath --import '$in{'file'}' 2>&1`;
```

Steps to reproduce:

1. `Usermin -> Tools -> File Manager -> File -> Create New File`

2. Filename must be command to run: `'; id '` this is because there is a check in `import.cgi` at line 19: `-r $in{'file'} || &error($text{'import_efile'});` to check if it is a valid file
3. `Usermin -> Applications -> GPG -> Manage Keys -> Import key (local file)`
4. Select the created file with command and import
5. Command is run as current user
6. Almost all chars except `/\` are valid

Email XSS - CVE-2022-36880

Type: XSS

JavaScript is not escaped properly in emails received

Steps to reproduce:

Receive email with the following html payload:

```
<iframe src=javascript&colon;alert&lpar;document&period;location&rpar;>
```

Webmin

Vulnerabilities for webmin 1.995 and prior.

Email XSS - CVE-2022-36880

Type: XSS

JavaScript is not escaped properly in emails received

Steps to reproduce:

Receive email with the following html payload:

1. Go to `Read user mail`
2. Press on email with payload bellow
3. Press `View` HTML document

```
<iframe src=javascript&colon;alert&lpar;document&period;location&rpar;>
```

Releases

No releases published

Packages

No packages published