



UNIVERSITÄT  
LEIPZIG



# ChatSEC: Spicing up Vulnerability Scans with AI for Heterogeneous University IT

Mario Hoffmann\*, **Erik Buchmann**<sup>†‡</sup>

buchmann@informatik.uni-leipzig.de

*1st International Conference on AI-based Systems  
and Services (AISyS 2024), Venice, Italy*

\* IT Department, Infrastructure Group, Leipzig University, Leipzig, Germany

† Department of Computer Science, Leipzig University, Germany

‡ Center for Scalable Data Analytics and Artificial Intelligence (ScaDS.AI),  
Dresden/Leipzig, Germany

# Someone is Taking out German Universities



## **Ransomware Attack Costs €1.7 Million**

December 2019: Ransomware attack forced Justus Liebig University Giessen to shut down email systems and servers, recovery took months.

## **Ransomware Shuts Down University's IT**

*May 2020: Ransomware led to the shutdown of large parts of the Ruhr University Bochum's IT infrastructure, disrupted academic activities for months.*

## **Death of a Patient due Delayed Treatment**

September 2020: Ransomware shut down the IT systems of University Hospital Düsseldorf, delayed treatment resulted in death of a patient.

## **Data from Employees and Students on the Dark Web**

April 2021: A Malware attack on Technical University of Berlin required to shut down IT systems and services, data from employees and students were leaked on the dark web.

## **MULTIPLE ATTACKS THROUGHOUT THE YEAR**

2023: Heinrich-Heine-Universität Düsseldorf was subject to multiple attacks. Again data from employees and students on the dark web.

# Typical Countermeasure: Vulnerability Scanners

## Vulnerability Scan Report

Scan Time: Wed, Jan 1, 2024 1:00 AM - Wed, Jan 1, 2024 1:09 AM, Hosts scanned: 1

### Results (1/1)

<i>Vulnerability</i>	<i>Severity</i>	<i>Host</i>	<i>Location</i>
Ubuntu: Security Advisory (USN-5767-1)	9.8 (High)	012.345.67.89	package

### Summary

The remote host is missing an update for the 'python2.7, python3.6, python3.8, python3.10' package(s).

### Vulnerability Detection Result

Vulnerable package: libpython3.8

Installed version: libpython3.8-3.8.10-0ubuntu1 20.04.5

Fixed version: >=libpython3.8-3.8.10-0ubuntu1 20.04.6

### Solution

Solution Type: Vendorfix. Please install the updated package(s).

### Affected Software/OS

'python2.7, python3.6, python3.8, python3.10' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 22.10.

### Vulnerability Insight

Nicky Mouha discovered that Python incorrectly handled certain SHA-3 internals. An attacker could possibly use this issue to cause a crash or execute arbitrary code. (CVE-2022-37454) Python incorrectly handled certain IDNA inputs. An attacker could possibly use this issue to expose sensitive information, denial of service, or cause a crash. (CVE-2022-45061)

### References

CVE: CVE-2022-37454 CVE-2022-45061 WID-SEC-2023-1007 WID-SEC-2023-0561 WID-SEC-2023-0255 WID-SEC-2023-0138 WID-SEC-2022-2043 WID-SEC-2022-1816 DFN-CERT-2023-1109 DFN-CERT-2023-0886 DFN-CERT-2023-0580 DFN-CERT-2023-0571 DFN-CERT-2023-0552 DFN-CERT-2023-0429 DFN-CERT-2023-0422 DFN-CERT-2023-0120 (⋯)

Other: <https://ubuntu.com/security/notices/USN-5767-1> advisory\_id:USN-5767-1

### Hosts 1 of 1

<i>IP-Address</i>	<i>Hostname</i>	<i>OS</i>	<i>High</i>	<i>Medium</i>	<i>Low</i>	<i>Total</i>	<i>Severity</i>
012.345.67.89	ourhost.ourdomain.tld	Canonical Ubuntu Linux	1	0	0	1	9.8 (High)

# Now the Real Fun Starts ;-)

- We are talking about universities...
  - Majority of vulnerabilities is on hosts in the research groups, local admins "inherit" responsibilities by chance
  - Students set up servers for exercises and forget them after the exam, PhD students set up demonstrators and leave to another university
  - Security fixes are postponed due to more pressing deadlines
  - Some research communities use outdated plain-text protocols, e.g., FTP
  - Due to academic self-administration, CIO and IT Department have limited authority to enforce security rules



# Our Contributions

- 1) We introduce ChatSEC, which uses an LLM to prepare vulnerability scans for people with limited cybersecurity knowledge
- 2) We discuss implementation alternatives to generate intuitive explanations, and to add threat intelligence and mitigation strategies
- 3) We provide a preliminary evaluation of ChatSEC

**Vulnerability Scan Report**  
Scan Time: Wed, Jan 1, 2024 1:00 AM - Wed, Jan 1, 2024 1:09 AM, Hosts scanned: 1

**Results (1/1)**

Vulnerability	Severity	Host	Location
Ubuntu: Security Advisory (USN-5767-1)	9.8 (High)	012.345.67.89	package

**Summary**  
The remote host is missing an update for the 'python2.7, python3.6, python3.8, python3.10' package(s).

**Vulnerability Detection Result**  
Vulnerable package: libpython3.8  
Installed version: libpython3.8-3.8.10-0ubuntu1 20.04.5  
Fixed version: >=libpython3.8-3.8.10-0ubuntu1 20.04.6

**Solution**  
Solution Type: Vendorfix. Please install the updated package(s).

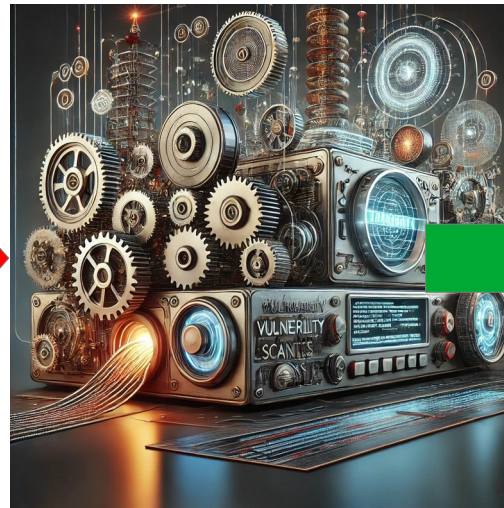
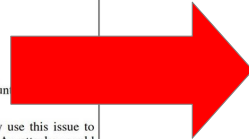
**Affected Software/OS**  
'python2.7, python3.6, python3.8, python3.10' package(s) on Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 24.04

**Vulnerability Insight**  
Nicky Mouha discovered that Python incorrectly handled certain SHA-3 internals. An attacker could possibly use this issue to cause a crash or execute arbitrary code. (CVE-2022-37454) Python incorrectly handled certain IDNA inputs. An attacker could possibly use this issue to expose sensitive information, denial of service, or cause a crash. (CVE-2022-45061)

**References**  
CVE: CVE-2022-37454 CVE-2022-45061 WID-SEC-2023-1007 WID-SEC-2023-0561 WID-SEC-2023-0255 WID-SEC-2023-0138 WID-SEC-2022-2043 WID-SEC-2022-1816 DFN-CERT-2023-1109 DFN-CERT-2023-0886 DFN-CERT-2023-0580 DFN-CERT-2023-0571 DFN-CERT-2023-0552 DFN-CERT-2023-0429 DFN-CERT-2023-0422 DFN-CERT-2023-0120 (...)  
Other: <https://ubuntu.com/security/notices/USN-5767-1> advisory\_id:USN-5767-1

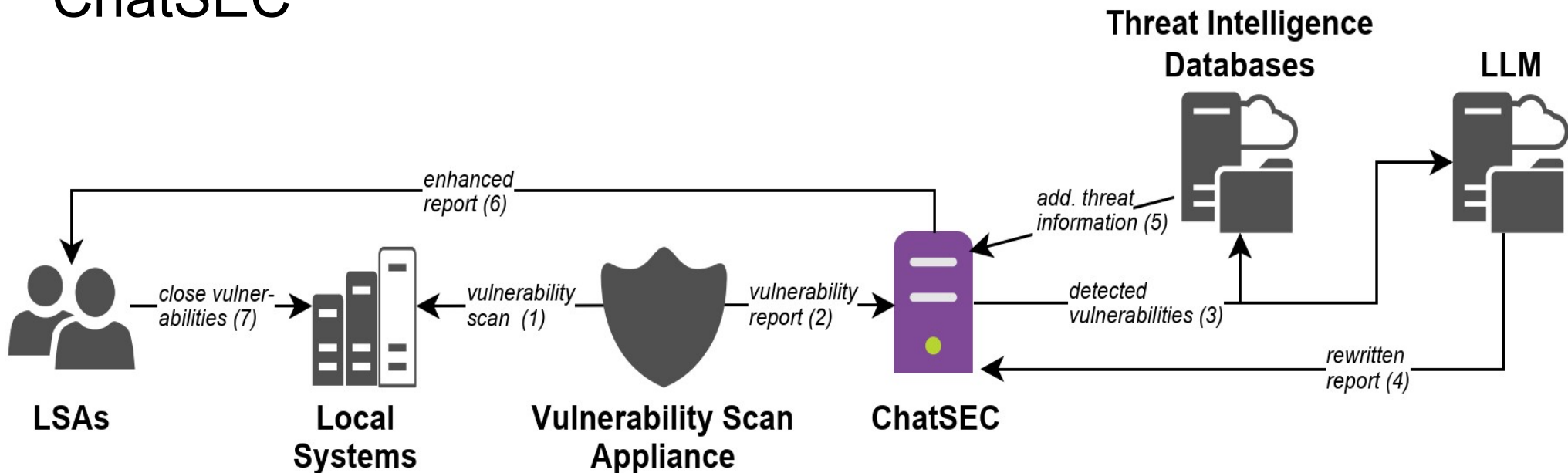
**Hosts 1 of 1**

IP-Address	Hostname	OS	High	Medium	Low	Total	Severity
012.345.67.89	ourhost.ourdomain.tld	Canonical Ubuntu Linux	1	0	0	1	9.8 (High)



*Dear Admin,  
please install the  
python update  
asap! An attacker  
could easily crash  
your Ubuntu  
system or execute  
harmful code.*

# ChatSEC



- 1) Run vulnerability scan on any local system
- 2) Send vulnerability scan to ChatSEC
- 3) Let LLM and Threat Intelligence DBs interpret detected vulnerabilities
- 4) Fetch rewritten report from LLM
- 5) Extend this report with treat intelligence
- 6) Send the final report to the Local System Administrator

# Example for a Rewritten Report

Reason for the report

*"This vulnerability description is about a security advisory for Ubuntu operating system. The advisory states that the **remote host** (a computer connected to a network) **is missing an update** for the 'python2.7, python3.6, python3.8, python3.10' packages. The update is announced in [Ubuntu Security Notice 767-1](#) advisory. The first vulnerability, identified as [CVE-2022-45060](#), is related to Python's handling of certain SHA-3 internals.*

What happens if this is ignored?

*This vulnerability could be exploited by an attacker to **cause a crash or execute arbitrary code** on the affected system. The second vulnerability, identified as [CVE-2022-45061](#), is related to Python's handling of certain IDNA inputs. An attacker could potentially exploit this vulnerability to **expose sensitive information**, perform a **denial of service attack**, or **cause a crash** on the affected system. In summary, these vulnerabilities in Python could allow attackers to crash the system, execute arbitrary code, expose sensitive information, or cause a denial of service attack.*

What has to be done?

*It is important to **update the affected packages** to protect the system from these potential risks."*

# Additional Threat Intelligence

- Threat Intelligence for CVE-ID *2019-0708*:
  - ***Searchsploit:*** 4 exploits already exist
  - ***CVE List:*** Root cause is "Use after Free"
  - ***National Vulnerability DB:***  
CVSSv3 score="9.8 (critical)",  
attackComplexity="low",  
privilegeRequired="None",  
userInteraction="None"



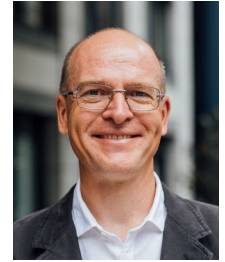
# Example for a Understandable Threat Intelligence

- LLM explains CVE ID 2019-0708
  - Searchsploit: 4 exploits already exist
  - CVE List: Root cause is "Use after Free"
  - National Vulnerability DB: CVSSv3 score=9.8 (critical), attackComplexity=low, privilegeRequired=None, userInteraction=None

*"The severity score indicates, that the attack complexity is low, meaning that it is relatively easy for an attacker to exploit the security vulnerability. Additionally, no privilege is required for the attack, meaning that the attacker does not need any special access rights or permissions to carry out the attack. Furthermore, there is no user interaction required, suggesting that the attack can be automated without user input. The referenced cause CWE-416, or "Use After Free," is a computer security vulnerability where a program tries to use memory that has already been freed up. This can cause errors or allow hackers to exploit the system. Searchsploit found 4 currently available exploits for this vulnerability."*

# Conclusion

- University is a cybersecurity challenge
- ChatSEC explains domain-specific vulnerabilities in plain-text language
- Our contributions
  - 1) ChatSEC, our approach to rewrite vulnerability scans
  - 2) Implementation alternatives for intuitive explanations, threat intelligence and mitigation strategies
  - 3) Preliminary evaluation of ChatSEC
- Future work
  - Gather feedback from YOU, and integrate ChatSEC into the next vulnerability scan at our university



Prof. Erik Buchmann

*Data Privacy and Security*

buchmann@informatik.uni-leipzig.de

## Example for a Rewritten Report

*"This vulnerability description is about a security advisory for Ubuntu operating system. The advisory states that the remote host (a computer connected to a network) is missing an update for the 'python2.7, python3.6, python3.8, python3.10' packages. The update is announced through the USN-5767-1 advisory. The first vulnerability, identified as CVE-2022-37454, is related to Python's handling of certain SHA-3 internals.*

*This vulnerability could be exploited by an attacker to cause a crash or execute arbitrary code on the affected system. The second vulnerability, identified as CVE-2022-45061, is related to Python's handling of certain IDNA inputs. An attacker could potentially exploit this vulnerability to expose sensitive information, perform a denial of service attack, or cause a crash on the affected system. In summary, these vulnerabilities in Python could allow attackers to crash the system, execute arbitrary code, expose sensitive information, or cause a denial of service attack.*

*It is important to update the affected packages to protect the system from these potential risks."*

# Example for Threat Intelligence

- LLM explains CVE ID 2019-0708
  - Searchsploit: 4 exploits already exist
  - CVE List: Root cause is "Use after Free"
  - National Vulnerability DB: CVSSv3 score=9.8 (critical), attackComplexity=low, privilegeRequired=None, userInteraction="None"

*"The severity score indicates, that the attack complexity is low, meaning that it is relatively easy for an attacker to exploit the security vulnerability. Additionally, no privilege is required for the attack, meaning that the attacker does not need any special access rights or permissions to carry out the attack. Furthermore, there is no user interaction required, suggesting that the attack can be automated without user input. The referenced cause CWE-416, or "Use After Free," is a computer security vulnerability where a program tries to use memory that has already been freed up. This can cause errors or allow hackers to exploit the system. Searchsploit found 4 currently available exploits for this vulnerability."*