Review and Confirm Your Submission

Your incident report has NOT yet been submitted. Please review and confirm your submission below.

To submit your report, please review the information below to verify the accuracy of the report and click the SUBMIT button. Or if you would like to revise your incident report you may click the EDIT buttons to return to the previous page.

Contact Information

Edit

Required fields are marked with an asterisk (*).

I am: *

- (•) The impacted user
- ( ) Reporting on behalf of the impacted user

Your Contact Information

First Name

first_name

Last Name

last_name

Telephone

Email *

11111111111

submitter@email.com

Organization Details

Edit

Required fields are marked with an asterisk (*).

The Impacted Organization's Details

What type of organization are you reporting for?*

Critical Infrastructure and/or Private Sector

Please enter the impacted organization's name or company name (please spell out any acronyms):*

organization_name

Please select the primary Critical Infrastructure sector that the impacted business is involved in:*

Information Technology

Please enter the impacted organization's internal tracking number (if applicable):

Incident Description

Edit

Required fields are marked with an asterisk (*).

Incident Description

When approximately, did the incident start? *

11/30/2024, 10:45 AM

When was this incident detected? *

12/02/2024, 10:45 AM

Please enter a brief description of the incident *

Account brute force attempts.

Impact Details

Edit

Required fields are marked with an asterisk (*).

Was the confidentiality, integrity, and/or availability of your organization's information systems potentially compromised? *

Additional questions may apply

- ○ Yes
- ◉ No

System Impact

Please define the functional impact to the organization by selecting one of the following *

Denial of Critical Services or Loss of Control

What is the number of systems impacted? *

1

How many users are impacted? *

100

How was this incident detected?

- ☐ Administrator
- ☐ User
- ☐ Anti-Virus (AV) Software
- ☐ Other
- ☐ Intrusion Detection System (IDS)
- ☐ Unknown
- ☑ Log Review

What operating systems (OS) are impacted?

Operating System #1

Operating System name

Windows 10

Operating System Version

Remove OS

Operating System #2

Operating System name

Linux OS

Operating System Version

Remove OS

+ Add Detail For Impacted OS

What is the function of the system(s) affected? Please select all that apply *

- [x] Application Server(s)
- [ ] Switch(es)
- [ ] Database Server(s)
- [ ] Time Server(s)
- [ ] Desktop(s)
- [ ] Web Server(s)
- [ ] Domain Name Server(s)
- [x] Laptop(s)
- [ ] Firewall(s)
- [ ] Other Server(s)
- [ ] ICS/SCADA System(s)
- [ ] Mail Server(s)
- [ ] Router(s)

Please Enter the Indicator Type

Indicator Type #1

Please Enter the Indicator Type

Host - Hash(es)

Indicators

d41d8cd98f00b204e9800998ecf8427e

Indicator Context

Remove Indicator

Indicator Type #2

Please Enter the Indicator Type

Host - Software meta-data

Indicators

Created: 2023-01-01 12:00:00 UTC

Indicator Context

Remove Indicator

Indicator Type #3

Please Enter the Indicator Type

Host - Software meta-data

Indicators

Adobe Reader 11.0.0

Indicator Context

Remove Indicator

Indicator Type #4

Please Enter the Indicator Type

Network - Email Address(es)

Indicators

user@example.com

Indicator Context

Remove Indicator

Indicator Type #5

Please Enter the Indicator Type

Network - Network Traffic

Indicators

TCP/443, UDP/53

Indicator Context

Remove Indicator

Indicator Type #6

Please Enter the Indicator Type

Host - X.509 Certificate(s)

Indicators

CN=*.example.com

Indicator Context

Remove Indicator

Indicator Type #7

Please Enter the Indicator Type

Network - URL

Indicators

https://malicious.example.com
malicious.company.com

Indicator Context

Remove Indicator

Indicator Type #8

Please Enter the Indicator Type

Network - Email Message(s)

Indicators

Email Message(s): Subject: "Important Update"

Indicator Context

Remove Indicator

Indicator Type #9

Please Enter the Indicator Type

Host - Mutex(es)

Indicators

\BaseNamedObjects\ExampleMutex

Indicator Context

Remove Indicator

Indicator Type #10

Please Enter the Indicator Type

Host - User Account(s)

Indicators

Administrator, Guest

Indicator Context

Remove Indicator

Indicator Type #11

Please Enter the Indicator Type

Host - System Processes

Indicators

svchost.exe, explorer.exe

Indicator Context

Remove Indicator

Indicator Type #12

Please Enter the Indicator Type

Host - Windows Registry

Indicators

HKEY_LOCAL_MACHINE\Software\Example

Indicator Context

Remove Indicator

Indicator Type #13

Please Enter the Indicator Type

Network - Domain Name(s)

Indicators

evil.example.com

Indicator Context

Remove Indicator

Indicator Type #14

Please Enter the Indicator Type

Network - Autonomous System(s) (AS)

Indicators

AS12345

Indicator Context

Remove Indicator

Indicator Type #15

Please Enter the Indicator Type

Host - File System Directory(ies)

Indicators

C:\Program Files\Example\

Indicator Context

Remove Indicator

Indicator Type #16

Please Enter the Indicator Type

Network - IPv6 Address(es)

Indicators

2001:db8::1234

Indicator Context

Remove Indicator

Indicator Type #17

Please Enter the Indicator Type

Network - IPv4 Address(es)

Indicators

192.168.1.1

Indicator Context

Remove Indicator

+ Add Indicator Type

Enter a Common Vulnerabilities and Exposure Identifier (CVE-ID).
Please do not include the CVE prefix (e.g., 2014-7654321):

2014-7654321

Observed Activity

Where was the activity observed *

Unknown

Characterize the observed activity at its most severe level *

Preparation

Impact Information

What is the known informational impact from the incident? *
Additional questions may apply

No Impact

Number of records impacted *

0

Recovery From Incident

Please select the organization's recoverability for this incident *
Additional questions may apply

Regular

Please enter the organization's estimated recovery time (rounded to the nearest whole number)

4

Unit

Hours

Please provide details here

Reset risky accounts

Does your agency currently consider this to be a breach that must be reported to Congress within 30 days in accordance with OMB Policy?

Yes No

Privacy Act Statement

Authority: 5 U.S.C. § 301 and 44 U.S.C. § 3101 authorize the collection of this information.

Purpose: The primary purpose for the collection of this information is to allow the Department of Homeland Security to contact you about your request.

Routine Uses: The information collected may be disclosed as generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act of 1974, as amended. This includes using the information as necessary and authorized by the routine uses published in DHS/ALL-002 - Department of Homeland Security (DHS) Mailing and Other Lists System November 25, 2008, 73 FR 71659.

Disclosure: Some entities are regulatory or statutorily required to submit incident reports to DHS, and those entities must provide information in this form as required by applicable statute, regulation, or similar mandate. Failure for provide this information may result in inaccurate record keeping of the entity's compliance. For non-mandatory incident reporting, providing this information is voluntary. However, failure to provide this information will prevent DHS from contacting you in the event there are questions about your report.

Save and Download Cancel Submit